NEC

# N8406-023 1Gb Intelligent L3 Switch

## Command Reference Guide (ISCLI)

Part number: 856-126757-304-00
Second edition: Oct 2007

PN# 456-01772-000

Legal notices

© 2007 NEC Corporation

The information contained herein is subject to change without notice. The only warranties for NEC products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. NEC shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

SunOS™ and Solaris™ are trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Cisco® is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Part number: 856-126757-304-00

Second edition: Oct 2007

# Contents


ISCLI Reference
- Introduction ... 8
- Additional references ... 8
- Connecting to the switch ... 8
  - Establishing a console connection ... 8
  - Setting an IP address ... 9
  - Establishing a Telnet connection ... 9
  - Establishing an SSH connection ... 9
- Accessing the switch ... 10
- Idle timeout ... 11
- Typographical conventions ... 11

ISCLI basics
- Introduction ... 13
- Accessing the ISCLI ... 13
- ISCLI Command Modes ... 13
- Global commands ... 14
- Command line interface shortcuts ... 15
  - Command abbreviation ... 15
  - Tab completion ... 15

Information Commands
- Introduction ... 16
- System Information commands ... 17
- SNMPv3 Information commands ... 17
  - SNMPv3 USM User Table information ... 18
  - SNMPv3 View Table information ... 18
  - SNMPv3 Access Table information ... 19
  - SNMPv3 Group Table information ... 20
  - SNMPv3 Community Table information ... 20
  - SNMPv3 Target Address Table information ... 21
  - SNMPv3 Target Parameters Table information ... 21
  - SNMPv3 Notify Table information ... 22
  - SNMPv3 dump ... 23
- System information ... 24
- Show recent syslog messages ... 25
- System user information ... 25
- Layer 2 information ... 26
- FDB information commands ... 27
  - Show all FDB information ... 27
  - Clearing entries from the forwarding database ... 27
- Link Aggregation Control Protocol information ... 28
  - LACP dump ... 28
- 802.1x information ... 29
- Spanning Tree information ... 30
- Rapid Spanning Tree and Multiple Spanning Tree information ... 32
- Common Internal Spanning Tree information ... 34
- Trunk group information ... 36
- VLAN information ... 36
- Layer 3 information ... 37
- Route information ... 37
  - Show all IP Route information ... 38
- ARP information ... 39
  - Show all ARP entry information ... 39
  - ARP address list information ... 39
- OSPF information ... 40
  - OSPF general information ... 41
  - OSPF interface information ... 41
  - OSPF Database information ... 42
  - OSPF route codes information ... 43
- Routing Information Protocol information ... 43
  - RIP Routes information ... 43

RIP user configuration ... 44
IP information ... 44
IGMP multicast group information ... 45
IGMP multicast router port information ... 45
VRRP information ... 46
802.1p information ... 47
ACL information ... 48
RMON Information ... 48
RMON history information ... 48
RMON alarm information ... 49
RMON event information ... 50
Link status information ... 51
Port information ... 52
Logical Port to GEA Port mapping ... 53
SFP information ... 53
Uplink Failure Detection information ... 54
Information dump ... 54

Statistics commands
Introduction ... 55
Port Statistics ... 55
802.1x statistics ... 56
Bridging statistics ... 58
Ethernet statistics ... 58
Interface statistics ... 60
Internet Protocol (IP) statistics ... 61
Link statistics ... 62
Port RMON statistics ... 62
Layer 2 statistics ... 64
FDB statistics ... 64
LACP statistics ... 64
Layer 3 statistics ... 65
IP statistics ... 66
Route statistics ... 67
ARP statistics ... 67
DNS statistics ... 67
ICMP statistics ... 68
TCP statistics ... 69
UDP statistics ... 70
IGMP Multicast Group statistics ... 70
OSPF statistics ... 71
OSPF global statistics ... 71
VRRP statistics ... 74
RIP statistics ... 75
GEA Layer 3 statistics ... 76
GEA Layer 3 statistics ... 76
Management Processor statistics ... 77
Packet statistics ... 77
TCP statistics ... 78
UDP statistics ... 78
CPU statistics ... 78
ACL statistics ... 79
SNMP statistics ... 79
NTP statistics ... 81
Uplink Failure Detection statistics ... 82
Statistics dump ... 82

Configuration Commands
Introduction ... 83
Viewing and saving changes ... 83
Saving the configuration ... 83
System configuration ... 84
System host log configuration ... 85
Secure Shell Server configuration ... 86
RADIUS server configuration ... 87
TACACS+ server configuration ... 88

NTP server configuration ..... 89
System SNMP configuration ..... 90
SNMPv3 configuration ..... 91
SNMPv3 User Security Model configuration ..... 92
SNMPv3 View configuration ..... 92
SNMPv3 View-based Access Control Model configuration ..... 93
SNMPv3 Group configuration ..... 93
SNMPv3 Community Table configuration ..... 94
SNMPv3 Target Address Table configuration ..... 94
SNMPv3 Target Parameters Table configuration ..... 95
SNMPv3 Notify Table configuration ..... 95
System Access configuration ..... 96
Management Networks configuration ..... 96
User Access Control configuration ..... 97
User ID configuration ..... 97
HTTPS Access configuration ..... 98
Port configuration ..... 99
Temporarily disabling a port ..... 100
Port link configuration ..... 100
ACL Port configuration ..... 100
Layer 2 configuration ..... 101
802.1x configuration ..... 101
802.1x Global configuration ..... 102
802.1x Port configuration ..... 103
Rapid Spanning Tree Protocol / Multiple Spanning Tree Protocol configuration ..... 104
Common Internal Spanning Tree configuration ..... 105
CIST bridge configuration ..... 105
CIST port configuration ..... 106
Spanning Tree configuration ..... 107
Bridge Spanning Tree configuration ..... 108
Spanning Tree port configuration ..... 109
Forwarding Database configuration ..... 110
Static FDB configuration ..... 110
Trunk configuration ..... 110
Layer 2 IP Trunk Hash configuration ..... 111
Link Aggregation Control Protocol configuration ..... 111
LACP Port configuration ..... 112
VLAN configuration ..... 112
Layer 3 configuration ..... 113
IP interface configuration ..... 113
Default Gateway configuration ..... 114
IP Static Route configuration ..... 114
Address Resolution Protocol configuration ..... 115
Static ARP configuration ..... 115
IP Forwarding configuration ..... 115
Network Filter configuration ..... 116
Route Map configuration ..... 117
IP Access List configuration ..... 118
Routing Information Protocol configuration ..... 119
RIP Interface configuration ..... 119
RIP Route Redistribution configuration ..... 120
Open Shortest Path First configuration ..... 121
OSFP Area Index configuration ..... 122
OSPF Summary Range configuration ..... 123
OSPF Interface configuration ..... 123
OSPF Virtual Link configuration ..... 124
OSPF Host Entry configuration ..... 124
OSPF Route Redistribution configuration ..... 125
OSPF MD5 Key configuration ..... 125
IGMP configuration ..... 126
IGMP snooping configuration ..... 126
IGMP static multicast router configuration ..... 127
IGMP filtering configuration ..... 127
IGMP filter definition ..... 127
IGMP filtering port configuration ..... 128

Domain Name System configuration ..... 128
Bootstrap Protocol Relay configuration ..... 128
Virtual Router Redundancy Protocol configuration ..... 129
VRRP Virtual Router configuration ..... 129
VRRP Virtual Router Priority Tracking configuration ..... 131
VRRP Virtual Router Group configuration ..... 131
VRRP Virtual Router Group Priority Tracking configuration ..... 132
VRRP Interface configuration ..... 133
VRRP Tracking configuration ..... 133
Quality of Service configuration ..... 134
QoS 802.1p configuration ..... 134
Access Control configuration ..... 135
Access Control List configuration ..... 135
ACL Ethernet Filter configuration ..... 135
ACL IP Version 4 Filter configuration ..... 136
ACL TCP/UDP Filter configuration ..... 137
ACL Packet Format configuration ..... 137
ACL Metering configuration ..... 138
ACL Re-mark configuration ..... 138
ACL Re-mark In-Profile configuration ..... 138
ACL Re-Mark Update User Priority configuration ..... 139
ACL Re-mark Out-of-Profile configuration ..... 139
ACL Group configuration ..... 139
Remote Monitoring configuration ..... 140
RMON history configuration ..... 140
RMON event configuration ..... 140
RMON alarm configuration ..... 141
Port mirroring ..... 142
Port-based port mirroring ..... 142
Uplink Failure Detection configuration ..... 143
Failure Detection Pair configuration ..... 143
Link to Monitor configuration ..... 143
Link to Disable configuration ..... 144
Configuration Dump ..... 145
Saving the active switch configuration ..... 145
Restoring the active switch configuration ..... 145

Operations Commands
Introduction ..... 146
Operations-level port options ..... 146
Operations-level port 802.1x options ..... 146
Operations-level VRRP options ..... 147

Boot Options
Introduction ..... 148
Updating the switch software image ..... 148
Downloading new software to the switch ..... 148
Selecting a software image to run ..... 149
Uploading a software image from the switch ..... 149
Selecting a configuration block ..... 150
Resetting the switch ..... 150
Accessing the AOS CLI ..... 151

Maintenance Commands
Introduction ..... 152
System maintenance ..... 152
Forwarding Database maintenance ..... 152
Debugging options ..... 153
ARP cache maintenance ..... 153
IGMP Snooping maintenance ..... 154
IGMP Mrouter maintenance ..... 154
Technical support dump ..... 154
TFTP/FTP technical support dump put ..... 154
Uuencode flash dump ..... 155
TFTP/FTP system dump put ..... 155
Clearing dump information ..... 155

Panic command ..... 156
Unscheduled system dumps ..... 156

# ISCLI Reference

## Introduction

The 1Gb Intelligent L3 Switch is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

The extensive switching software included in the switch provides a variety of options for accessing and configuring the switch:

- Text-based command line interfaces (AOS CLI and ISCLI) for access via a local terminal or remote Telnet/Secure Shell (SSH) session
- Simple Network Management Protocol (SNMP) support for access through network management software such as NEC WebSAM NetvisorPro
- A browser-based management interface for interactive network access through a Web browser

The ISCLI provides a direct method for collecting switch information and performing switch configuration. Use a basic terminal to view information and statistics about the switch, and to perform any necessary configuration.

This chapter explains how to access the ISCLI to the switch.

## Additional references

Additional information about installing and configuring the switch is available in the following guides, which are attached in this product.

- *N8406-023 1Gb Intelligent L3 Switch User's Guide*
- *N8406-023 1Gb Intelligent L3 Switch Application Guide*
- *N8406-023 1Gb Intelligent L3 Switch Command Reference Guide (AOS)*
- *N8406-023 1Gb Intelligent L3 Switch Browser-based Interface Reference Guide*

## Connecting to the switch

You can access the command line interface in one of the following ways:

- Using a console connection via the console port
- Using a Telnet connection over the network
- Using a Secure Shell (SSH) connection to securely log in over a network

### Establishing a console connection

To establish a console connection with the switch, you need:

- A null modem cable with a female DB-9 connector (See the *N8406-023 1Gb Intelligent L3 Switch User's Guide* for more information.)
- An ASCII terminal or a computer running terminal emulation software set to the parameters shown in the table below

Table 1 Console configuration parameters

| Parameter | Value |
|---|---|
| Baud Rate | 9600 |
| Data Bits | 8 |
| Parity | None |
| Stop Bits | 1 |
| Flow Control | None |

To establish a console connection with the switch:

1. Connect the terminal to the console port using the null modem cable.
2. Power on the terminal.
3. Press the Enter key a few times on the terminal to establish the connection.
4. You will be required to enter a password for access to the switch.

## Setting an IP address

To access the switch via a Telnet or an SSH connection, you need to have an Internet Protocol (IP) address set for the switch. The switch can get its IP address in one of the following ways:

- Management port access:
  - Using a Dynamic Host Control Protocol (DHCP) server—When the `dhcp` client is `enabled`, the management interface (interface 256) requests its IP address from a DHCP server. The default value for the dhcp client is `enabled`.
  - Configuring manually—If the network does not support DHCP, you must configure the management interface (interface 256) with an IP address. If you want to access the switch from a remote network, you also must configure the management gateway (gateway 4).
- Uplink port access:
  - Using a Bootstrap Protocol (BOOTP) server—By default, the management interface is set up to request its IP address from a BOOTP server. If you have a BOOTP server on the network, add the Media Access Control (MAC) address of the switch to the BOOTP configuration file located on the BOOTP server. The MAC address can be found in the System Information menu (See the “System Information commands” section in the “Information Commands” chapter.) If you are using a DHCP server that also does BOOTP, you do not have to configure the MAC address.
  - Configuring manually—If the network does not support BOOTP, you must configure the management port with an IP address.

## Establishing a Telnet connection

A Telnet connection offers the convenience of accessing the switch from any workstation connected to the network. Telnet provides the same options for user, operator, and administrator access as those available through the console port. By default, Telnet is enabled on the switch. The switch supports four concurrent Telnet connections.

Once the IP parameters are configured, you can access the ISCLI using a Telnet connection. To establish a Telnet connection with the switch, run the Telnet program on the workstation and enter the telnet command, followed by the switch IP address:

```
telnet <1Gb Intelligent L3 Switch IP address>
```

You will then be prompted to enter a password. The password determines the access level: administrator, operator, or user. See the “Accessing the switch” section later in this chapter for description of default passwords.

## Establishing an SSH connection

Although a remote network administrator can manage the configuration of a switch via Telnet, this method does not provide a secure connection. The Secure Shell (SSH) protocol enables you to securely log into this switch over the network.

As a secure alternative to using Telnet to manage switch configuration, SSH ensures that all data sent over the network is encrypted and secure. In order to use SSH, you must first configure it on the switch. See the “Secure Shell Server configuration” section in the “Configuration Commands” chapter for information on how to configure SSH.

The switch can perform only one session of key/cipher generation at a time. Therefore, an SSH/Secure Copy (SCP) client will not be able to log in if the switch is performing key generation at that time or if another client has just logged in before this client. Similarly, the system will fail to perform the key generation if an SSH/SCP client is logging in at that time.

The supported SSH encryption and authentication methods are listed below.

- Server Host Authentication—Client RSA authenticates the switch in the beginning of every connection
- Key Exchange—RSA
- Encryption:
  - AES256-CBC
  - AES192-CBC
  - AES128-CBC
  - 3DES-CBC
  - 3DES
  - ARCFOUR
- User Authentication—Local password authentication; Remote Authentication Dial-in User Service (RADIUS)

The following SSH clients are supported:

- SSH 3.0.1 for Linux (freeware)
- SecureCRT® 4.1.8 (VanDyke Technologies, Inc.)
- OpenSSH_3.9 for Linux (FC 3)
- FedoraCore 3 for SCP commands
- PuTTY Release 0.58 (Simon Tatham) for Windows

NOTE: This switch implementation of SSH is based on versions 1.5 and 2.0, and supports SSH clients from version 1.0 through version 2.0. SSH clients of other versions are not supported. You may configure the client software to use protocol SSH version 1 or version 2.

By default, SSH service is not enabled on the switch. Once the IP parameters are configured, you can access the ISCLI to enable SSH.

To establish an SSH connection with the switch, run the SSH program on the workstation by issuing the ssh command, followed by the user account name and the switch IP address:

```
>> # ssh <user>@<1Gb Intelligent L3 Switch IP address>
```

You will then be prompted to enter your password.

NOTE: The first time you run SSH from the workstation, a warning message might appear. At the prompt, enter yes to continue.

# Accessing the switch

To enable better switch management and user accountability, this switch provides different levels or classes of user access. Levels of access to the CLI and Web management functions and screens increase as needed to perform various switch management tasks. The three levels of access are:

- User— Interaction with the switch is completely passive—nothing can be changed on this switch. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- Operator— Interaction with the switch is completely passive—nothing can be changed on this switch. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- Administrator— Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reload/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on this switch. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique usernames and passwords. Once you are connected to the switch via the local console, Telnet, or SSH, you are prompted to enter a password. The password entered determines the access level. The default user names/password for each access level is listed in the following table.

NOTE: It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies. For more information, see the “Setting passwords” section in the “First-time configuration” chapter.

Table 2 User access levels

| User account | Description and tasks performed |
|---|---|
| User | The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch. The user account is enabled by default, and the default password is `user`. |
| Oper | The Operator has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch. By default, the operator account is disabled and has no password. |
| Admin | The super user administrator has complete access to all command modes on the switch, including the ability to change both the user and administrator passwords. The admin account is enabled by default, and the default password is `admin`. |

NOTE: With the exception of the admin user, access to each user level can be disabled by setting the password to an empty value.

Once you enter the administrator password and it is verified, you are given complete access to this switch.

# Idle timeout

By default, this switch disconnects the console, Telnet, or SSH session after five minutes of inactivity. This function is controlled by the idle timeout parameter, which can be set from 1 to 60 minutes. To change this parameter, see the “System configuration” section in the “Configuration Commands” chapter.

# Typographical conventions

The following table describes the typographic styles used in this guide:

| Typeface or symbol | Meaning |
|---|---|
| angle brackets < > | Indicate a variable to enter based on the description inside the brackets. Do not type the brackets as you enter the command.<br>Example: If the command syntax is<br>**`ping <`***`IP address`***`>`**<br><br>you enter<br>`ping 192.32.10.12` |
| bold body text | Indicates objects, such as window names, icons, and user-interface objects, such as buttons and tabs. |
| `bold Courier text` | Indicates command names, options, and text that you must enter.<br>Example:<br>Use the **`show ip arp`** commands. |
| `plain Courier text` | Indicates command syntax and system output (for example: prompts and system messages). Example:<br>`configure terminal` |
| braces { } | Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.<br>Example: If the command syntax is<br>**`show portchannel {<`***`1-12`***`>\|hash\|information}`**<br><br>you must enter:<br>`show portchannel <1-12>`<br><br>or<br>`show portchannel hash`<br><br>or<br>`show portchannel information` |

| Typeface or symbol | Meaning |
|---|---|
| brackets [ ] | Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.<br>Example: If the command syntax is<br>**show ip interface [<*1-256*>]**<br><br>you can enter<br>`show ip interface`<br><br>or<br>`show ip interface 1` |
| *italic text* | Indicates variables in command syntax descriptions. Also indicates new terms and book titles. Where a variable is two or more words, the words are connected by a hyphen.<br>Example: If the command syntax is<br>**show spanning-tree stp <***1-32***>**<br><br>1-32 represents a number between 1-32. |
| vertical line \| | Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.<br>Example: If the command syntax is<br>**show portchannel {<***1-12***>\|hash\|information}**<br><br>you must enter:<br>`show portchannel <1-12>`<br><br>or<br>`show portchannel hash`<br><br>or<br>`show portchannel information` |

# ISCLI basics

## Introduction

The ISCLI is used for viewing switch information and statistics. In addition, the administrator can use the CLI for performing all levels of switch configuration.

This chapter describes the ISCLI Command Modes, and provides a list of commands and shortcuts that are commonly available from all the command modes within the ISCLI.

## Accessing the ISCLI

The first time you start this switch, it boots into the AOS CLI. To access the ISCLI, enter the following command and reset the switch:

```
Main# boot/mode iscli
```

To access the AOS CLI, enter the following command from the ISCLI and reload the switch:

```
Switch(config)# boot cli-mode aos
```

The switch retains your CLI selection, even when you reset the configuration to factory defaults. The CLI boot mode is not part of the configuration settings.

## ISCLI Command Modes

The ISCLI has three major command modes, listed in order of increasing privileges, as follows:

User EXEC mode: This is the initial mode of access. By default, password checking is disabled for this mode.

Privileged EXEC mode: The mode is accessed from User EXEC mode. If the Privileged EXEC password is enabled, you must enter a password to access Privileged EXEC mode.

Global Configuration mode: This mode allows you to make changes to the running configuration of the switch. If you save the configuration, the settings survive a reload of the switch. Several submodes are available within the Global Configuration mode (the following table for more information.

Each command mode provides a specific set of commands. The command set of each higher-privilege mode is a superset of the lower-privilege mode(s). All commands available in lower-lower-privilege modes are available in the higher-privilege modes.

The following table describes the ISCLI command modes.

Table 3 ISCLI Command Modes

| Command Mode/Prompt | Command used to enter or exit. |
|---|---|
| User EXEC<br><br>`Switch>` | Default mode, entered automatically<br>Exit: **`exit`** or **`logout`** |
| Privileged EXEC<br><br>`Switch#` | Enter Privileged EXEC mode, from User EXEC mode: **`enable`**<br>Exit to User EXEC mode: **`disable`**<br>Quit ISCLI: **`exit`** or **`logout`** |
| Global configuration<br><br>`Switch(config)#` | Enter Global Configuration mode, from Privileged EXEC mode:<br>**`configure terminal`**<br>Exit to Privileged EXEC mode: **`end`** or **`exit`** |
| Port configuration<br><br>`Switch(config-if)#` | Enter Port Configuration mode, from Global Configuration mode:<br>**`interface gigabitethernet <`***`port number`***`>`**<br>Exit to Global Configuration mode: **`exit`**<br>Exit to Privileged EXEC mode: **`end`** |
| VLAN configuration<br><br>`Switch(config-vlan)#` | Enter VLAN Configuration mode, from Global Configuration mode: **`vlan <`***`1-4095`***`>`**<br>Exit to Global Configuration mode: **`exit`**<br>Exit to Privileged EXEC mode: **`end`** |
| Interface IP configuration<br><br>`Switch(config-ip-if)#` | Enter Interface IP Configuration mode, from Global Configuration mode:<br>**`interface ip <`***`1-256`***`>`**<br>Exit to Global Configuration mode: **`exit`**<br>Exit to Privileged EXEC mode: **`end`** |

Table 3 ISCLI Command Modes

| Command Mode/Prompt | Command used to enter or exit. |
|---|---|
| RIP configuration<br><br>`Switch(config-router-rip)#` | Enter RIP Configuration mode, from Global Configuration mode: **`router rip`**<br>Exit to Global Configuration mode: **`exit`**<br>Exit to Privileged EXEC mode: **`end`** |
| OSPF configuration<br><br>`Switch(config-router-ospf)#` | Enter OSPF Configuration mode, from Global Configuration mode: **`router ospf`**<br>Exit to Global Configuration mode: **`exit`**<br>Exit to Privileged EXEC mode: **`end`** |
| VRRP configuration<br><br>`Switch(config-vrrp)#` | Enter VRRP Configuration mode, from Global Configuration mode: **`router vrrp`**<br>Exit to Global Configuration mode: **`exit`**<br>Exit to Privileged EXEC mode: **`end`** |
| Route-map configuration<br><br>`Switch(config-route-map)#` | Enter Route-map Configuration mode, from Global Configuration mode: **`route-map`** *<1-32>*<br>Exit to Global Configuration mode: **`exit`**<br>Exit to Privileged EXEC mode: **`end`** |
| FDP configuration<br><br>`Switch(config-fdp)#` | Enter RIP Configuration mode, from Global Configuration mode: **`ufd fdp`** *<1-4>*<br>Exit to Global Configuration mode: **`exit`**<br>Exit to Privileged EXEC mode: **`end`** |

# Global commands

Some basic commands are recognized throughout the ISCLI hierarchy. These commands are useful for obtaining online Help, navigating through the interface, and saving configuration changes. To get help about a specific command, type the command, followed by **`help`**.

The following table describes the global commands.

Table 4 Global commands

| Command | Action |
|---|---|
| `?` | Provides more information about a specific command or lists commands available at the current level. |
| `exit` | Go up one level in the command-mode structure. |
| `copy running-config startup-config` | Write configuration changes to non-volatile flash memory. |
| `exit or quit` | Exit from the command line interface and log out. |
| `ping` | Verify station-to-station connectivity across the network. The format is as follows:<br>`ping` *<host name> \| <IP address>* `[`*<number of tries>*`] [`*<msec delay>*`]`<br>• IP address is the hostname or IP address of the device.<br>• number of tries (optional) is the number of attempts (1-32).<br>• msec delay (optional) is the number of milliseconds between attempts. |
| `traceroute` | Identifies the route used for station-to-station connectivity across the network. The format is as follows:<br>`traceroute` *<host name> \| <IP address>* `[`*<max-hops>*`] [`*<msec delay>*`]`<br>• IP address is the hostname or IP address of the target station.<br>• max-hops (optional) is the maximum distance to trace (1-16 devices)<br>• msec delay (optional) is the number of milliseconds to wait for the response. |
| `telnet` | Allows you to Telnet out of the switch. The format is as follows:<br>`telnet` *<host name> \| <IP address>* `[`*<port number>*`]` |
| `show history` | Displays the 10 most recent commands. |
| `console-log` | Enables or disables console logs for the current session. |
| `who` | Displays a list of users who are currently logged in. |

# Command line interface shortcuts

The following shortcuts allow you to enter commands quickly and easily.

## Command abbreviation

Most commands can be abbreviated by entering the first characters that distinguish the command from the others in the same mode. For example, consider the following full command:

```
Switch(config)# spanning-tree stp 1 bridge hello-time 2
```

The command shown above could also be entered as:

```
Switch(config)# sp stp 1 br h 2
```

## Tab completion

Entering the first letter of a command at any prompt and press the Tab key to display all available commands or options that begin with that letter. Entering additional letters further refines the list of commands or options displayed.

If only one command fits the input text when you press the Tab key, that command is supplied on the command line, waiting to be entered.

# Information Commands

## Introduction

You can view configuration information for the switch in the ISCLI. This chapter discusses how to use the ISCLI to display switch information.

The following table describes general information commands.

Table 5 Information commands

| Command | Usage |
|---|---|
| **show sys-info** | Displays system information.<br>**Command mode**: All |
| **show layer2 information** | Displays Layer 2 information.<br>**Command mode**: All |
| **show layer3 information** | Displays Layer 3 information.<br>**Command mode**: All |
| **show rmon** | Displays Remote Monitoring Information.<br>**Command mode**: All |
| **show interface link** | Displays configuration information about each port, including:<br>• Port number<br>• Port speed (10 Mb/s, 100 Mb/s, 1000 Mb/s, or any)<br>• Duplex mode (half, full, or any)<br>• Flow control for transmit and receive (no, yes, or any)<br>• Link status (up or down)<br>**Command mode**: All |
| **show interface information** | Displays port status information, including:<br>• Port number<br>• Whether the port uses VLAN tagging or not<br>• Port VLAN ID (PVID)<br>• Port name<br>• VLAN membership<br>**Command mode**: All |
| **show geaport** | Displays GEA port mapping information, used by service personnel.<br>**Command mode**: All |
| **show sfp** | Displays SFP module information.<br>**Command mode**: All |
| **show ufd** | Displays Uplink Failure Detection information.<br>**Command mode**: All |
| **show information-dump** | Dumps all switch information available (10K or more, depending on your configuration).<br>If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.<br>**Command mode**: All |

# System Information commands

The following table describes the System Information commands.

Table 6 System Information commands

| Command | Usage |
|---|---|
| **show snmp-server v3** | Displays SNMP v3 information.<br>**Command mode**: All |
| **show sys-info** | Displays system information, including:<br>• System date and time<br>• Switch model name and number<br>• Switch name and location<br>• Time of last boot<br>• MAC address of the switch management processor<br>• IP address of IP interface #1<br>• Hardware version and part number<br>• Software image file and version number<br>• Configuration name<br>• Log-in banner, if one is configured<br>**Command mode**: All |
| **show logging messages** | Displays most recent syslog messages.<br>**Command mode**: All |
| **show access user** | Displays User Access information.<br>**Command mode**: All except User EXEC |

# SNMPv3 Information commands

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture, see RFC2271 to RFC2276.

The following table describes the SNMPv3 Information commands.

Table 7 SNMPv3 Information commands

| Command | Usage |
|---|---|
| **show snmp-server v3 user** | Displays User Security Model (USM) table information.<br>**Command mode**: All |
| **show snmp-server v3 view** | Displays information about view name, subtrees, mask and type of view.<br>**Command mode**: All |
| **show snmp-server v3 access** | Displays View-based Access Control information.<br>**Command mode**: All |
| **show snmp-server v3 group** | Displays information about the group that includes the security model, user name, and group name.<br>**Command mode**: All |
| **show snmp-server v3 community** | Displays information about the community table.<br>**Command mode**: All |
| **show snmp-server v3 target-address** | Displays the Target Address table.<br>**Command mode**: All |
| **show snmp-server v3 target-parameters** | Displays the Target parameters table.<br>**Command mode**: All |
| **show snmp-server v3 notify** | Displays the Notify table.<br>**Command mode**: All |
| **show snmp-server v3** | Displays all the SNMPv3 information.<br>**Command mode**: All |

## SNMPv3 USM User Table information

The following command displays SNMPv3 user information:

**show snmp-server v3 user**

**Command mode:** All

```
usmUser Table
User Name                       Protocol
------------------------------- --------------------------------
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
v1v2only                        NO AUTH,  NO PRIVACY
```

The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. This security model makes use of a defined set of user identities displayed in the USM user table. The USM user table contains information like:

- the user name
- a security name in the form of a string whose format is independent of the Security Model
- an authentication protocol, which is an indication that the messages sent on behalf of the user can be authenticated
- the privacy protocol.

The following table describes the SNMPv3 User Table information.

Table 8 User Table parameters

| Field | Description |
|---|---|
| `User Name` | This is a string that represents the name of the user that you can use to access the switch. |
| `Protocol` | This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. switch software supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA. |

## SNMPv3 View Table information

The following command displays the SNMPv3 View Table:

**show snmp-server v3 view**

**Command mode:** All

```
View Name          Subtree                      Mask           Type
------------------ ---------------------------  -------------  --------
iso                  1                                        included
v1v2only             1                                        included
v1v2only             1.3.6.1.6.3.15                           excluded
v1v2only             1.3.6.1.6.3.16                           excluded
v1v2only             1.3.6.1.6.3.18                           excluded
```

The user can control and restrict the access allowed to a group to only a subset of the management information in the management domain that the group can access within each context by specifying the group's rights in terms of a particular MIB view for security reasons.

The following table describes the SNMPv3 View Table information.

Table 9 View Table parameters

| Field | Description |
|---|---|
| View Name | Displays the name of the view. |
| Subtree | Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names. |
| Mask | Displays the bit mask. |
| Type | Displays whether a family of view subtrees is included or excluded from the MIB view. |

## SNMPv3 Access Table information

The following command displays SNMPv3 access information:

**show snmp-server v3 access**

**Command mode:** All

```
Group Name  Model   Level         ReadV     WriteV   NotifyV
----------  ------- ------------ --------- -------- -------
v1v2grp     snmpv1  noAuthNoPriv iso        iso     v1v2only
admingrp    usm     authPriv     iso        iso     iso
```

The access control sub system provides authorization services.

The vacmAccessTable maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view.

The View-based Access Control Model defines a set of services that an application can use for checking access rights of a group. This group's access rights are determined by a read-view, a write-view, and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification.

The following table describes the SNMPv3 Access Table information.

Table 10 Access Table parameters

| Field | Description |
|---|---|
| Group Name | Displays the name of group. |
| Model | Displays the security model used, for example, SNMPv1, or SNMPv2 or USM. |
| Level | Displays the minimum level of security required to gain rights of access. For example, noAuthNoPriv, authNoPriv, or auth-Priv. |
| ReadV | Displays the MIB view to which this entry authorizes the read access. |
| WriteV | Displays the MIB view to which this entry authorizes the write access. |
| NotifyV | Displays the Notify view to which this entry authorizes the notify access. |

## SNMPv3 Group Table information

The following command displays SNMPv3 group information:

**show snmp-server v3 group**

**Command mode:** All

```
Sec Model  User Name                     Group Name
---------- ---------------------------- --------------------------------
snmpv1     v1v2only                     v1v2grp
usm        adminmd5                     admingrp
usm        adminsha                     admingrp
```

A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name.

The following table describes the SNMPv3 Group Table information.

Table 11 Group Table parameters

| Field | Description |
|---|---|
| Sec Model | Displays the security model used, which is any one of: USM, SNMPv1, SNMPv2, and SNMPv3. |
| User Name | Displays the name for the user. |
| Group Name | Displays the access name of the group. |

## SNMPv3 Community Table information

The following command displays SNMPv3 community information:

**show snmp-server v3 community**

**Command mode:** All

```
Index      Name       User Name            Tag
---------- ---------- -------------------- ----------
trap1      public     v1v2only             v1v2trap
```

This command displays the community table information stored in the SNMP engine.

The following table describes the SNMPv3 Community Table information.

Table 12 Community Table information

| Field | Description |
|---|---|
| Index | Displays the unique index value of a row in this table. |
| Name | Displays the community string, which represents the configuration. |
| User Name | Displays the User Security Model (USM) user name. |
| Tag | Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap. |

## SNMPv3 Target Address Table information

The following command displays SNMPv3 target address information:

**show snmp-server v3 target-address**

**Command mode:** All

```
Name       Transport Addr  Port Taglist    Params
---------- --------------- ---- ---------- ---------------
trap1      47.81.25.66     162  v1v2trap   v1v2param
```

This command displays the SNMPv3 target address table information, which is stored in the SNMP engine.

The following table describes the SNMPv3 Target Address Table information.

Table 13 Target Address Table information

| Field | Description |
|---|---|
| Name | Displays the locally arbitrary, but unique identifier associated with this snmpTargetAddrEntry. |
| Transport Addr | Displays the transport addresses. |
| Port | Displays the SNMP UDP port number. |
| Taglist | This column contains a list of tag values which are used to select target addresses for a particular SNMP message. |
| Params | The value of this object identifies an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address. |

## SNMPv3 Target Parameters Table information

The following command displays SNMPv3 target parameters information:

**show snmp-server v3 target-parameters**

**Command mode:** All

```
Name                MP Model User Name            Sec Model Sec Level
------------------- -------- -------------------- --------- -----------
v1v2param            snmpv2c  v1v2only             snmpv1    noAuthNoPriv
```

The following table describes the SNMPv3 Target Parameters Table information.

Table 14 Target Parameters Table information

| Field | Description |
|---|---|
| Name | Displays the locally arbitrary, but unique identifier associated with this snmpTargeParamsEntry. |
| MP Model | Displays the Message Processing Model used when generating SNMP messages using this entry. |
| User Name | Displays the securityName, which identifies the entry on whose behalf SNMP messages will be generated using this entry. |
| Sec Model | Displays the security model used when generating SNMP messages using this entry. The system may choose to return an inconsistentValue error if an attempt is made to set this variable to a value for a security model which the system does not support. |
| Sec Level | Displays the level of security used when generating SNMP messages using this entry. |

## SNMPv3 Notify Table information

The following command displays the SNMPv3 Notify Table:

**`show snmp-server v3 notify`**

**Command mode:** All

```
Name                 Tag
-------------------- --------------------
v1v2trap             v1v2trap
```

The following table describes the SNMPv3 Notify Table information.

Table 15 SNMPv3 Notify Table information

| Field | Description |
|---|---|
| `Name` | The locally arbitrary, but unique identifier associated with this snmpNotifyEntry. |
| `Tag` | This represents a single tag value which is used to select entries in the `snmpTargetAddrTable`. Any entry in the `snmpTargetAddrTable` that contains a tag value equal to the value of this entry is selected. If this entry contains a value of zero length, no entries are selected. |

## SNMPv3 dump

The following command displays SNMPv3 information:

**show snmp-server v3**

**Command mode:** All

```
Engine ID = 80:00:07:50:03:00:0F:6A:F8:EF:00
usmUser Table:
User Name                       Protocol
------------------------------- -------------------------------
admin                           NO AUTH, NO PRIVACY
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
v1v2only                        NO AUTH, NO PRIVACY

vacmAccess Table:
Group Name Prefix Model   Level        ReadV   WriteV   NotifyV
---------- ------ ------- ------------ ------- -------- ------
admin             usm     noAuthNoPriv org     org      org
v1v2grp           snmpv1  noAuthNoPriv org     org      v1v2only
admingrp          usm     authPriv     org     org      org

vacmViewTreeFamily Table:
View Name            Subtree         Mask         Type
-------------------- --------------- ------------ --------------
org                  1.3                          included
v1v2only             1.3                          included
v1v2only             1.3.6.1.6.3.15               excluded
v1v2only             1.3.6.1.6.3.16               excluded
v1v2only             1.3.6.1.6.3.18               excluded

vacmSecurityToGroup Table:
Sec Model  User Name                       Group Name
---------- ------------------------------- ----------------------
snmpv1     v1v2only                        v1v2grp
usm        admin                           admin
usm        adminsha                        admingrp

snmpCommunity Table:
Index      Name       User Name            Tag
---------- ---------- -------------------- ----------

snmpNotify Table:
Name                 Tag
-------------------- --------------------

snmpTargetAddr Table:
Name       Transport Addr  Port Taglist    Params
---------- --------------- ---- ---------- ---------------

snmpTargetParams Table:
Name                 MP Model User Name          Sec Model Sec Level
-------------------- -------- ------------------ --------- -------
```

# System information

The following command displays system information:

**`show sys-info`**

**Command mode:** All

```
System Information at  6:56:22 Thu Jan 11, 2006
Time zone: Asia/Tokyo

Blade Network Technologies 1Gb Intelligent L3 Switch
sysName:
sysLocation:
RackId: NEC01A 6X00125
RackName: Default_Rack_Name
EnclosureSerialNumber: NEC01A 6X00125
EnclosureName: Default_Chassis_Name
BayNumber:  1

Switch is up 0 days, 14 hours, 56 minutes and 22 seconds.
Last boot: 17:25:38 Mon Jan 8, 2006 (software reset)

MAC address: 00:10:00:01:00:01    IP (If 1) address: 10.14.4.16
Revision:
Switch Serial No:
Spare Part No:
Software Version 1.0.0 (FLASH image2), active configuration.
```

System information includes:

- System date and time
- Switch model name and number
- Rack name and location
- Time of last boot
- MAC address of the switch management processor
- IP address of the switch
- Software image file and version number
- Current configuration block (active, backup, or factory default)
- Login banner, if one is configured

# Show recent syslog messages

The following command displays system log messages:

**`show logging messages`**

**Command mode:** All

```
Date   Time            Severity level                  Message
----   ----         -----------------                  -------
Jul 8 17:25:41             NOTICE              system: link up on port 1
Jul 8 17:25:41             NOTICE              system: link up on port 8
Jul 8 17:25:41             NOTICE              system: link up on port 7
Jul 8 17:25:41             NOTICE              system: link up on port 12
Jul 8 17:25:41             NOTICE              system: link up on port 11
Jul 8 17:25:41             NOTICE              system: link up on port 14
Jul 8 17:25:41             NOTICE              system: link up on port 13
Jul 8 17:25:41             NOTICE              system: link up on port 16
Jul 8 17:25:41             NOTICE              system: link up on port 15
Jul 8 17:25:41             NOTICE              system: link up on port 17
Jul 8 17:25:41             NOTICE              system: link up on port 20
Jul 8 17:25:41             NOTICE              system: link up on port 22
Jul 8 17:25:41             NOTICE              system: link up on port 23
Jul 8 17:25:41             NOTICE              system: link up on port 21
Jul 8 17:25:42             NOTICE              system: link up on port 4
Jul 8 17:25:42             NOTICE              system: link up on port 3
Jul 8 17:25:42             NOTICE              system: link up on port 6
Jul 8 17:25:42             NOTICE              system: link up on port 5
Jul 8 17:25:42             NOTICE              system: link up on port 10
Jul 8 17:25:42             NOTICE              system: link up on port 9
```

Each message contains a date and time field and has a severity level associated with it. One of eight different prefixes is used to indicate the condition:

- EMERG—indicates the system is unusable
- ALERT—indicates action should be taken immediately
- CRIT—indicates critical conditions
- ERR—indicates error conditions or eroded operations
- WARNING—indicates warning conditions
- NOTICE—indicates a normal but significant condition
- INFO—indicates an information message
- DEBUG—indicates a debug-level message

# System user information

The following command displays user status information:

**`show access user`**

**Command mode:** All except User EXEC

```
Usernames:
  user     - enabled
  oper     - disabled
  admin    - Always Enabled

Current User ID table:
  1: name tech1   , ena, cos user    , password valid, online
  2: name tech2   , ena, cos user    , password valid, offline
```

The following table describes the user status information.

Table 16 User status Information

| Field | Usage |
|---|---|
| `user` | Displays the status of the `user` access level. |
| `oper` | Displays the status of the `oper` (operator) access level. |
| `admin` | Displays the status of the `admin` (administrator) access level. |
| `Current User ID Table` | Displays the status of configured user IDs. |

# Layer 2 information

The following table describes the Layer 2 Information commands. The following sections provide more detailed information and commands.

Table 17 Layer 2 information commands

| Command | Usage |
|---|---|
| **show mac-address-table** | Displays Forwarding Database Information.<br>**Command mode**: All |
| **show lacp information** | Displays a summary of LACP information.<br>**Command mode**: All |
| **show qos transmit-queue information** | Displays 802.1p Information.<br>**Command mode**: All |
| **show dot1x information** | Displays 802.1x Information.<br>**Command mode**: All |
| **show spanning-tree stp** *<1-128>* **information** | In addition to seeing if STP is enabled or disabled, you can view the following STP bridge information:<br>• Priority<br>• Hello interval<br>• Maximum age value<br>• Forwarding delay<br>• Aging time<br>You can also refer to the following port-specific STP information:<br>• Port number and priority<br>• Cost<br>• State<br>**Command mode**: All |
| **show spanning-tree mstp cist information** | Displays Common internal Spanning Tree (CIST) bridge information, including the following:<br>• Priority<br>• Hello interval<br>• Maximum age value<br>• Forwarding delay<br>You can also view port-specific CIST information, including the following:<br>• Port number and priority<br>• Cost<br>• State<br>**Command mode**: All |
| **show portchannel information** | When trunk groups are configured, you can view the state of each port in the various trunk groups.<br>**Command mode**: All |
| **show vlan information** | Displays VLAN configuration information, including:<br>• VLAN Number<br>• VLAN Name<br>• Status<br>• Port membership of the VLAN<br>**Command mode**: All |
| **show layer2 information** | Dumps all switch information available from Layer 2 memory (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.<br>**Command mode**: All |

# FDB information commands

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

NOTE: The master forwarding database supports up to 8K MAC address entries on the management processor (MP) per switch.

Table 18 FDB information commands

| | |
|---|---|
| **show mac-address-table address** *<mac-address>* | Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device.<br>Enter the MAC address using the format: xx:xx:xx:xx:xx:xx. (For example: 08:00:20:12:34:56)<br>You can also enter the MAC address using the format: xxxxxxxxxxxx. (For example: 080020123456)<br>**Command mode**: All |
| **show mac-address-table port** *<port number>* | Displays all FDB entries for a particular port.<br>**Command mode**: All |
| **show mac-address-table vlan** *<1-4095>* | Displays all FDB entries on a single VLAN. The range is 1-4095.<br>**Command mode**: All |
| **show mac-address-table state {forward\|trunk\|unknown}** | Displays all FDB entries that match a particular state.<br>**Command mode**: All |
| **show mac-address-table** | Displays all entries in the Forwarding Database.<br>**Command mode**: All |

## Show all FDB information

The following command displays Forwarding Database information:

**show mac-address-table**

**Command mode:** All

```
   MAC address      VLAN  Port  Trnk  State
-----------------  ----  ----  ----  -----
00:02:01:00:00:00   300          1    TRK
00:02:01:00:00:01   300   23           FWD
00:02:01:00:00:02   300   23           FWD
00:02:01:00:00:03   300   23           FWD
00:02:01:00:00:04   300   23           FWD
00:02:01:00:00:05   300   23           FWD
00:02:01:00:00:06   300   23           FWD
00:02:01:00:00:07   300   23           FWD
00:02:01:00:00:08   300   23           FWD
00:02:01:00:00:09   300   23           FWD
00:02:01:00:00:0a   300   23           FWD
00:02:01:00:00:0b   300   23           FWD
00:02:01:00:00:0c   300   23           FWD
```

An address that is in the forwarding (FWD) state indicates that the switch has learned it. When in the trunking (TRK) state, the Trnk field displays the trunk group number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address. When an address is in the unknown state, no outbound port is indicated.

## Clearing entries from the forwarding database

To delete a static MAC address from the forwarding database (FDB), see the “Static FDB configuration” section in the “Configuration Commands” chapter.

# Link Aggregation Control Protocol information

The following table describes the Link Aggregation Control Protocol information commands.

Table 19 LACP information commands

| Command | Usage |
|---|---|
| **show interface gigabitEthernet <***port number***> lacp information** | Displays LACP aggregator information for the port.<br>**Command mode**: All |
| **show lacp** | Displays LACP information for the port.<br>**Command mode**: All |
| **show lacp information** | Displays all LACP information parameters.<br>**Command mode**: All |

## LACP dump

The following command displays LACP information:

**show lacp information**

**Command mode:** All

```
>> LACP# dump
port  lacp      adminkey  operkey  selected    prio    attached  trunk
                                                          aggr
------------------------------------------------------------------------
   1  off             1        1         n    32768        --     --
   2  off             2        2         n    32768        --     --
   3  off             3        3         n    32768        --     --
   4  off             4        4         n    32768        --     --
   5  off             5        5         n    32768        --     --
   6  off             6        6         n    32768        --     --
   7  off             7        7         n    32768        --     --
   8  off             8        8         n    32768        --     --
```

LACP dump includes the following information for each port in the switch:

- lacp—Displays the port's LACP mode (active, passive, or off)
- adminkey—Displays the value of the port's adminkey.
- operkey—Shows the value of the port's operational key.
- selected—Indicates whether the port has been selected to be part of a Link Aggregation Group.
- prio—Shows the value of the port priority.
- attached aggr—Displays the aggregator associated with each port.
- trunk—This value represents the LACP trunk group number.

# 802.1x information

The following command displays 802.1x information:

**`show dot1x information`**

**Command mode:** All

```
System capability : Authenticator
System status     : disabled
Protocol version  : 1
                                      Authenticator    Backend
Port   Auth Mode    Auth Status     PAE State     Auth State
----  ------------  ------------  --------------  ----------
 1    force-auth    unauthorized  initialize      initialize
 2    force-auth    unauthorized  initialize      initialize
 3    force-auth    unauthorized  initialize      initialize
 4    force-auth    unauthorized  initialize      initialize
 5    force-auth    unauthorized  initialize      initialize
 6    force-auth    unauthorized  initialize      initialize
 7    force-auth    unauthorized  initialize      initialize
 8    force-auth    unauthorized  initialize      initialize
 9    force-auth    unauthorized  initialize      initialize
 10   force-auth    unauthorized  initialize      initialize
 11   force-auth    unauthorized  initialize      initialize
 12   force-auth    unauthorized  initialize      initialize
 13   force-auth    unauthorized  initialize      initialize
 14   force-auth    unauthorized  initialize      initialize
 15   force-auth    unauthorized  initialize      initialize
 16   force-auth    unauthorized  initialize      initialize
*17   force-auth    unauthorized  initialize      initialize
*18   force-auth    unauthorized  initialize      initialize
 19   force-auth    unauthorized  initialize      initialize
 20   force-auth    unauthorized  initialize      initialize
*21   force-auth    unauthorized  initialize      initialize
 22   force-auth    unauthorized  initialize      initialize
*23   force-auth    unauthorized  initialize      initialize
*24   force-auth    unauthorized  initialize      initialize
------------------------------------------------------------------------
* - Port down or disabled
```

The following table describes the IEEE 802.1x parameters.

Table 20 802.1x information

| Field | Description |
|---|---|
| `Port` | Displays each port's name. |
| `Auth Mode` | Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following:<br>• force-unauth<br>• auto<br>• force-auth |
| `Auth Status` | Displays the current authorization status of the port, either authorized or unauthorized. |
| `Authenticator PAE State` | Displays the Authenticator Port Access Entity State. The PAE state can be one of the following:<br>• initialize<br>• disconnected<br>• connecting<br>• authenticating<br>• authenticated<br>• aborting<br>• held<br>• forceAuth |

Table 20 802.1x information

| Field | Description |
|---|---|
| `Backend Auth State` | Displays the Backend Authorization State. The Backend Authorization state can be one of the following:<br>• initialize<br>• request<br>• response<br>• success<br>• fail<br>• timeout<br>• idle |

# Spanning Tree information

The following table describes the Spanning Tree Protocol (STP) information commands.

Table 21 STP information commands

| Command | Usage |
|---|---|
| **show spanning-tree stp** *<1-128>* | Displays information about the spanning tree group.<br>**Command mode**: All |
| **show spanning-tree stp** *<1-128>* **bridge** | Displays STP bridge information.<br>**Command mode**: All |
| **show spanning-tree stp** *<1-128>* **information** | Displays STP information.<br>**Command mode**: All |
| **show spanning-tree** | Displays all STP information.<br>**Command mode**: All |

The following command displays Spanning Tree information:

**show spanning-tree**

**Command mode:** All

```
--------------------------------------------------------------------

upfast disabled, update 40
--------------------------------------------------------------------


Spanning Tree Group 1: On (STP/PVST+)
VLANs: 1

Current Root:            Path-Cost    Port  Hello MaxAge FwdDel
 8000 00:02:a5:d1:0f:ed        8       20    2     20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32768      2      20      15     300

Port  Priority   Cost   FastFwd    State       Designated Bridge     Des Port
----  --------   ----   --------  ----------   --------------------- -------
  1         0      0       n      FORWARDING *
  2         0      0       n      FORWARDING *
  3         0      0       n      FORWARDING *
```

The switch software uses the IEEE 802.1D Spanning Tree Protocol (STP). If RSTP/MSTP is turned on, see the “Rapid Spanning Tree information” section for Spanning Tree Group information. In addition to seeing if STP is enabled or disabled, you can view the following STP bridge information:

- Status of Uplink Fast (upfast)
- Current root MAC address
- Path cost
- Port
- Hello interval

- Maximum age value
- Forwarding delay
- Aging time

You can also refer to the following port-specific STP information:

- Port number and priority
- Cost
- State
- Port Fast Forwarding state
- Designated bridge
- Designated port

The following table describes the STP parameters.

Table 22 STP parameters

| Parameter | Description |
|---|---|
| `Current Root` | Shows information about the root bridge for the Spanning Tree. Information includes the priority (hex) and MAC address of the root. |
| `Path-Cost` | Path-cost is the total path cost to the root bridge. It is the summation of the path cost between bridges (up to the root bridge). |
| `Port` | The current root port refers to the port on the switch that receives data from the current root. Zero (0) indicates the root bridge of the STP. |
| `Priority (bridge)` | The bridge priority parameter controls which bridge on the network will become the STP root bridge. |
| `Hello` | The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. |
| `MaxAge` | The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. If the bridge is not the root bridge, it uses the `MaxAge` value of the root bridge. |
| `FwdDel` | The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state. If the bridge is not the root bridge, it uses the `FwdDel` value of the root bridge. |
| `Aging` | The aging time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database. |
| `Priority (port)` | The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. |
| `Cost` | The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. |
| `State` | The State field shows the current state of the port. The State field can be one of the following: `BLOCKING`, `LISTENING`, `LEARNING`, `FORWARDING`, or `DISABLED`. |
| `Designated bridge` | Shows information about the bridge connected to each port, if applicable. Information includes the priority (hex) and MAC address of the Designated Bridge. |
| `Designated port` | The port ID of the port on the Designated Bridge to which this port is connected. This information includes the port priority (hex) and the port number (hex). |

# Rapid Spanning Tree and Multiple Spanning Tree information

The following command displays RSTP/MSTP information:

**`show spanning-tree`**

**Command mode:** All

```
---------------------------------------------------------------
upfast disabled, update 40
---------------------------------------------------------------
Spanning Tree Group 1: On (RSTP)
VLANs: 1-3 4095

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 8000 00:00:01:00:19:00        0       0    9     20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32768      9      20      15     300

Port  Prio  Cost   State  Role    Designated Bridge   Des Port  Type
----  ----  ----  ------  ----  -------------------- --------  ----
  1     0       0     DSB
  2     0       0     DSB
  3     0       0     DSB
  4     0       0     DSB
  5     0       0     DSB
  6     0       0     DSB
  7     0       0     DSB
  8     0       0     DSB
  9     0       0     DSB
 10     0       0     DISC
 11     0       0     FWD   DESG 8000-00:00:01:00:19:00   8017  P2P2,Edge
 12     0       0     FWD   DESG 8000-00:00:01:00:19:00   8018  P2P
```

The switch software can be set to use the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). If RSTP/MSTP is turned on, you can view the following RSTP bridge information for the Spanning Tree Group:

- Status of Uplink Fast (upfast)
- Current root MAC address
- Path-Cost
- Port
- Hello interval
- Maximum age value
- Forwarding delay
- Aging time

You can also refer to the following port-specific RSTP information:

- Port number and priority
- Cost
- State
- Role
- Designated bridge and port
- Link type

The following table describes the STP parameters in RSTP or MSTP mode.

Table 23 Rapid Spanning Tree parameter descriptions

| Parameter | Description |
|---|---|
| `Current Root` | Shows information about the root bridge for the Spanning Tree. Information includes the priority (hex) and MAC address of the root. |
| `Path-Cost` | Path-cost is the total path cost to the root bridge. It is the summation of the path cost between bridges (up to the root bridge). |
| `Port` | The current root port refers to the port on the switch that receives data from the current root. Zero (0) indicates the root bridge of the STP. |
| `Priority (bridge)` | The bridge priority parameter controls which bridge on the network will become the STP root bridge. |
| `Hello` | The hello time parameter specifies, in seconds, how often the root bridge transmits a configurationbridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. |
| `MaxAge` | The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. If the bridge is not the root bridge, it uses the `MaxAge` value of the root bridge. |
| `FwdDel` | The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state. If the bridge is not the root bridge, it uses the `FwdDel` value of the root bridge. |
| `Aging` | The aging time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database. |
| `Priority (port)` | The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. |
| `Cost` | The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of zero (0) indicates that the cost will be set to the appropriate default after the link speed has been auto-negotiated. |
| `State` | Shows the current state of the port. The State field in RSTP/MSTP mode can be one of the following: `Discarding (DISC)`, `Learning (LRN)`, `Forwarding (FWD)`, or `Disabled (DSB)`. |
| `Role` | Shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Master (MAST), or Unknown (UNK). |
| `Designated bridge` | Shows information about the bridge connected to each port, if applicable. Information includes the priority (hex) and MAC address of the Designated Bridge. |
| `Designated port` | The port ID of the port on the Designated Bridge to which this port is connected. |
| `Type` | Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED. |

# Common Internal Spanning Tree information

The following command displays Common Internal Spanning Tree (CIST) information:

**`show spanning-tree mstp cist information`**

**Command mode:** All

```
Mstp Digest: 0xac36177f50283cd4b83821d8ab26de62
Common Internal Spanning Tree:
VLANs: 1 3-4094

Current Root:            Path-Cost  Port   MaxAge   FwdDel
 8000 00:03:42:fa:3b:80      11     1       20      15

CIST Regional Root:    Path-Cost
 8000 00:03:42:fa:3b:80       11

Parameters:  Priority  MaxAge  FwdDel  Hops
               32768      20      15    20

Port Prio Cost State  Role Designated Bridge     Des Port Hello Type
---- ---- ---- ------ ---- -------------------- -------- ----- ----
  1  128  2000   FWD  DESG 8000-00:03:42:fa:3b:80  8001     4   P2P,Edge
  2  128  2000   FWD  DESG 8000-00:03:42:fa:3b:80  8002
  3  128  2000   DSB
  4  128  2000   DSB
  5  128  2000   DSB
  6  128  2000   DSB
  7  128  2000   DSB
  8  128  2000   DSB
  9  128  2000   DSB
 10  128  0      DSB
 11  128  2000   FWD   DESG 8000-00:03:42:fa:3b:80
 12  128  2000   DSB
```

In addition to seeing if Common Internal Spanning Tree (CIST) is enabled or disabled, you can view the following CIST bridge information:

- CIST root
- CIST regional root
- Priority
- Maximum age value
- Forwarding delay
- Hops

You can also refer to the following port-specific CIST information:

- Port number and priority
- Cost
- State
- Role
- Designated bridge and port
- Hello interval
- Link type and port type

The following table describes the CIST parameters.

Table 24 Common Internal Spanning Tree parameter descriptions

| Parameter | Description |
|---|---|
| CIST Root | Shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root. |
| CIST Regional Root | Shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root. |
| Priority (bridge) | The bridge priority parameter controls which bridge on the network will become the STP root bridge. |
| MaxAge | The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. |
| FwdDel | The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state. |
| Hops | Shows the maximum number of bridge hops allowed before a packet is dropped. |
| Priority (port) | The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. |
| Cost | The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of zero (0) indicates that the cost will be set to the appropriate default after the link speed has been auto-negotiated. |
| State | Shows the current state of the port. The state field can be one of the following: Discarding (DISC), Learning (LRN), Forwarding (FWD), or Disabled (DSB). |
| Role | Shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Master (MAST), or Unknown (UNK). |
| Designated Bridge | Shows information about the bridge connected to each port, if applicable. Information includes the priority (hex) and MAC address of the Designated Bridge. |
| Designated Port | The port ID of the port on the Designated Bridge to which this port is connected. Information includes the port priority (hex) and the port number (hex). |
| Hello | The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. |
| Type | Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED. |

# Trunk group information

The following command displays Trunk Group information:

**show portchannel information**

**Command mode:** All

```
Trunk group 1, Enabled
port state:
  17: STG  1 forwarding
  18: STG  1 forwarding
```

When trunk groups are configured, you can view the state of each port in the various trunk groups.

NOTE: If Spanning Tree Protocol on any port in the trunk group is set to forwarding, the remaining ports in the trunk group are set to forwarding.

# VLAN information

The following table describes the VLAN information commands.

Table 25 VLAN information commands

| Command | Usage |
|---|---|
| **show vlan** | Displays VLAN information<br>**Command mode**: All |
| **show vlan information** | Displays VLAN information, including spanning tree assignment.<br>**Command mode**: All |

The following command displays VLAN information:

**show vlan information**

**Command mode:** All

```
VLAN                Name                Status  Ports
----  --------------------------------- ------  ----------------
1     Default VLAN                        ena    4  5
2     pc03p                               ena    2
7     pc07f                               ena    7
11    pc04u                               ena    11
14    8600-14                             ena    14
15    8600-15                             ena    15
16    8600-16                             ena    16
17    8600-17                             ena    17
18    35k-1                               ena    18
20    35k-3                               ena    20
21    35k-4                               ena    21
22    pc07z                               ena    22
24    redlan                              ena    24
300   ixiaTraffic                         ena    1 12 13 23
4000  bpsports                            ena    3-6 8-10
4095  Mgmt VLAN                           ena    19
```

This information display includes all configured VLANs and all member ports that have an active link state.

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN

# Layer 3 information

The following table describes basic Layer 3 Information commands. The following sections provide more detailed information and commands.

Table 26 Layer 3 information commands

| Command | Usage |
|---|---|
| **show ip route** | Displays all routes configured in the switch.<br>**Command mode**: All except User EXEC |
| **show ip information** | Displays general IP information.<br>**Command mode**: All except User EXEC |
| **show ip arp** | Displays Address Resolution Protocol (ARP) Information.<br>**Command mode**: All except User EXEC |
| **show ip ospf information** | Displays the OSPF information.<br>**Command mode**: All except User EXEC |
| **show interface ip** *<1-256>* **rip** | Displays RIP user's configuration.<br>**Command mode**: All except User EXEC |
| **show layer3 information** | Displays IP Information. IP information, includes:<br>• IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status.<br>• Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status<br>• IP forwarding information: Enable status, Inet and Imask<br>• Port status<br>**Command mode**: All except User EXEC |
| **show ip igmp groups** | Displays IGMP Information.<br>**Command mode**: All except User EXEC |
| **show ip vrrp information** | Displays the VRRP Information.<br>**Command mode**: All except User EXEC |
| **show layer3** | Dumps all switch information available from Layer 3 memory (10K or more, depending on your configuration).<br>If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.<br>**Command mode**: All except User EXEC |

# Route information

Using the commands listed below, you can display all or a portion of the IP routes currently held in the switch.

Table 27 Route Information commands

| Command | Usage |
|---|---|
| **show ip route address <***IP address***>** | Displays a single route by destination IP address.<br>**Command mode**: All except User EXEC |
| **show ip route gateway <***IP address***>** | Displays routes to a single gateway.<br>**Command mode**: All except User EXEC |
| **show ip route type {indirect\|direct\|local\|broadcast\|martian\|multicast}** | Displays routes of a single type.<br>**Command mode**: All except User EXEC |
| **show ip route tag {fixed\|static\|address\|rip\|ospf\|broadcast\|multicast\|martian}** | Displays routes of a single tag.<br>**Command mode**: All except User EXEC |
| **show ip route interface <***1-256***>** | Displays routes on a single interface.<br>**Command mode**: All except User EXEC |
| **show ip route** | Displays all routes configured in the switch.<br>**Command mode**: All except User EXEC |

# Show all IP Route information

The following command displays IP route information:

**show ip route**

**Command mode:** All except User EXEC

```
Status code: * - best
Destination        Mask           Gateway         Type      Tag       Metr If
---------------  --------------- --------------- --------- --------- ---- --
* 11.0.0.0       255.0.0.0       11.0.0.1        direct    fixed          211
* 11.0.0.1       255.255.255.255 11.0.0.1        local     addr           211
* 11.255.255.255 255.255.255.255 11.255.255.255  broadcast broadcast      211
* 12.0.0.0       255.0.0.0       12.0.0.1        direct    fixed          12
* 12.0.0.1       255.255.255.255 12.0.0.1        local     addr           12
* 12.255.255.255 255.255.255.255 12.255.255.255  broadcast broadcast      12
* 13.0.0.0       255.0.0.0       11.0.0.2        indirect  ospf      2    211
* 47.0.0.0       255.0.0.0       47.133.88.1     indirect  static         24
* 47.133.88.0    255.255.255.0   47.133.88.46    direct    fixed          24
* 172.30.52.223  255.255.255.255 172.30.52.223   broadcast broadcast 2
* 224.0.0.0      224.0.0.0       0.0.0.0         martian   martian
* 224.0.0.5      255.255.255.255 0.0.0.0         multicast addr
```

The following table describes the `Type` parameter.

Table 28 IP Routing Type information

| Field | Description |
|---|---|
| `indirect` | The next hop to the host or subnet destination will be forwarded through a router at the `Gateway` address. |
| `direct` | Packets will be delivered to a destination host or subnet attached to the switch. |
| `local` | Indicates a route to one of the switch's IP interfaces. |
| `broadcast` | Indicates a broadcast route. |
| `martian` | The destination belongs to a host or subnet which is filtered out. Packets to this destination are discarded. |
| `multicast` | Indicates a multicast route. |

The following table describes the `Tag` parameter.

Table 29 IP Routing Tag information

| Field | Description |
|---|---|
| `fixed` | The address belongs to a host or subnet attached to the switch. |
| `static` | The address is a static route which has been configured on the Switch. |
| `addr` | The address belongs to one of the switch's IP interfaces. |
| `rip` | The address was learned by the Routing Information Protocol (RIP). |
| `ospf` | The address was learned by Open Shortest Path First (OSPF). |
| `broadcast` | Indicates a broadcast address. |
| `martian` | The address belongs to a filtered group. |

# ARP information

The Address Resolution Protocol (ARP) information includes IP address and MAC address of each entry, address status flags, VLAN, and port for the address, and port referencing information.

The following table describes the Address Resolution Protocol commands.

Table 30 ARP information

| Command | Usage |
|---|---|
| **show ip arp find** *<IP address>* | Displays a single ARP entry by IP address.<br>**Command mode**: All except User EXEC |
| **show ip arp interface** *<port number>* | Displays the ARP entries on a single port.<br>**Command mode:** All except User EXEC |
| **show ip arp vlan** *<1-4095>* | Displays the ARP entries on a single VLAN.<br>**Command mode**: All except User EXEC |
| **show ip arp** | Displays all ARP entries, including:<br>• IP address and MAC address of each entry<br>• Address status flag<br>• The VLAN and port to which the address belongs<br>The ports which have referenced the address (empty if no port has routed traffic to the IP address shown)<br>**Command mode**: All except User EXEC |
| **show ip arp reply** | Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.<br>**Command mode**: All except User EXEC |

## Show all ARP entry information

The following command displays ARP information:

**show ip arp**

**Command mode:** All except User EXEC

```
IP address      Flags     MAC address               VLAN      Port
--------------- -----    -----------------          ----      ----
192.168.2.4             00:50:8b:b2:32:cb          1         18
192.168.2.19            00:0e:7f:25:89:b5          1         17
192.168.2.61    P       00:0f:6a:ed:46:00          1
```

The Flag field provides additional information about an entry. If no flag displays, the entry is normal.

Table 31 ARP dump flag parameters

| Flag | Description |
|---|---|
| P | Permanent entry created for switch IP interface. |
| R | Indirect route entry. |
| U | Unresolved ARP entry. The MAC address has not been learned. |

## ARP address list information

The following command displays ARP address list information:

**show ip arp reply**

**Command mode:** All except User EXEC

```
  IP address        IP mask        MAC address     VLAN Flags
--------------- ---------------  ----------------- ---- -----
205.178.18.66   255.255.255.255  00:70:cf:03:20:04 4095
205.178.50.1    255.255.255.255  00:70:cf:03:20:04    1
```

# OSPF information

The following table describes the OSPF commands.

Table 32 OSPF information commands

| Command | Usage |
|---|---|
| **show ip ospf general-information** | Displays general OSPF information.<br>**Command mode**: All except User EXEC |
| **show ip ospf area information [<*0-2*>]** | Displays area information for a particular area index. If no parameter is supplied, it displays area information for all the areas.<br>**Command mode**: All except User EXEC |
| **show ip ospf interface** | Displays interface information.<br>**Command mode**: All except User EXEC |
| **show ip ospf area-virtual-link information** | Displays information about all the configured virtual links.<br>**Command mode**: All except User EXEC |
| **show ip ospf neighbor** | Displays the status of all the current neighbors.<br>**Command mode**: All except User EXEC |
| **show ip ospf summary-range <*0-2*>** | Displays the list of summary ranges belonging to non-NSSA areas.<br>**Command mode**: All except User EXEC |
| **show ip ospf summary-range-nssa <*0-2*>** | Displays the list of summary ranges belonging to NSSA areas.<br>**Command mode**: All except User EXEC |
| **show ip ospf routes** | Displays OSPF routing table.<br>**Command mode**: All except User EXEC |
| **show ip ospf information** | Displays the OSPF information.<br>**Command mode**: All except User EXEC |

## OSPF general information

The following command displays general OSPF information:

**`show ip ospf general-information`**

**Command mode:** All except User EXEC

```
OSPF Version 2
Router ID: 10.10.10.1
Started at 1663 and the process uptime is 4626
Area Border Router: yes, AS Boundary Router: no
LS types supported are 6
External LSA count 0
External LSA checksum sum 0x0
Number of interfaces in this router is 2
Number of virtual links in this router is 1
16 new lsa received and 34 lsa originated from this router
Total number of entries in the LSDB 10
Database checksum sum 0x0
Total neighbors are 1, of which
                                2 are >=INIT state,
                                2 are >=EXCH state,
                                2 are =FULL state
Number of areas is 2, of which 3-transit 0-nssa
        Area Id : 0.0.0.0
        Authentication : none
        Import ASExtern : yes
        Number of times SPF ran : 8
        Area Border Router count : 2
        AS Boundary Router count : 0
        LSA count : 5
        LSA Checksum sum : 0x2237B
        Summary : noSummary
```

## OSPF interface information

The following command displays OSPF interface information:

**`show ip ospf interface`**

**Command mode:** All except User EXEC

```
Ip Address 10.10.12.1, Area 0.0.0.1, Admin Status UP
   Router ID 10.10.10.1, State DR, Priority 1
   Designated Router (ID) 10.10.10.1, Ip Address 10.10.12.1
   Backup Designated Router (ID) 10.10.14.1, Ip Address 10.10.12.2
   Timer intervals, Hello 10, Dead 40, Wait 1663, Retransmit 5,
   Transit delay 1
   Neighbor count is 1 If Events 4, Authentication type none
```

# OSPF Database information

The following table describes the OSPF Database information commands.

Table 33 OSPF Database information commands

| Command | Usage |
|---|---|
| **show ip ospf database advertising-router <*router ID*>** | Takes advertising router as a parameter. Displays all the Link State Advertisements (LSAs) in the LS database that have the advertising router with the specified router ID, for example: 20.1.1.1.<br>**Command mode**: All except User EXEC |
| **show ip ospf database asbr-summary [advertising-router <*router ID*> \|link-state-id <*A.B.C.D*> \| self]** | Displays ASBR summary LSAs. The usage of this command is as follows:<br>a. show ip ospf database asbr-summary advertising-router 20.1.1.1 displays ASBR summary LSAs having the advertising router 20.1.1.1.<br>b. show ip ospf database asbr-summary link_state_id 10.1.1.1 displays ASBR summary LSAs having the link state ID 10.1.1.1.<br>c. show ip ospf database asbr-summary self displays the self advertised ASBR summary LSAs.<br>d. this command with no parameters displays all the ASBR summary LSAs.<br>**Command mode**: All except User EXEC |
| **show ip ospf database database-summary** | Displays the following information about the LS database in a table format:<br>a. The number of LSAs of each type in each area.<br>b. The total number of LSAs for each area.<br>c. The total number of LSAs for each LSA type for all areas combined.<br>d. The total number of LSAs for all LSA types for all areas combined.<br>No parameters are required.<br>**Command mode**: All except User EXEC |
| **show ip ospf database external [advertising-router <*router ID*> \|link-state-id <*A.B.C.D*> \| self]** | Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs.<br>**Command mode**: All except User EXEC |
| **show ip ospf database network [advertising-router <*router ID*> \|link-state-id <*A.B.C.D*> \| self]** | Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database.<br>**Command mode**: All except User EXEC |
| **show ip ospf database nssa [advertising-router <*router ID*> \|link-state-id <*A.B.C.D*> \| self]** | Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs.<br>**Command mode**: All except User EXEC |
| **show ip ospf database router [advertising-router <*router ID*> \|link-state-id <*A.B.C.D*> \| self]** | Displays the router (type 1) LSAs with detailed information of each field of the LSAs.<br>**Command mode**: All except User EXEC |
| **show ip ospf database self** | Displays all the self-advertised LSAs. No parameters are required.<br>**Command mode**: All except User EXEC |
| **show ip ospf database summary [advertising-router <*router ID*> \| linkstate-id <*A.B.C.D*> \| self]** | Displays the network summary (type 3) LSAs with detailed information of each field of the LSAs.<br>**Command mode**: All except User EXEC |
| **show ip ospf database** | Displays all the LSAs.<br>**Command mode**: All except User EXEC |

## OSPF route codes information

The following command displays OSPF route information:

**show ip ospf routes**

**Command mode:** All except User EXEC

```
Codes: IA - OSPF inter area,
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
IA 10.10.0.0/16 via 200.1.1.2
IA 40.1.1.0/28 via 20.1.1.2
IA 80.1.1.0/24 via 200.1.1.2
IA 100.1.1.0/24 via 20.1.1.2
IA 140.1.1.0/27 via 20.1.1.2
IA 150.1.1.0/28 via 200.1.1.2
E2 172.18.1.1/32 via 30.1.1.2
E2 172.18.1.2/32 via 30.1.1.2
E2 172.18.1.3/32 via 30.1.1.2
E2 172.18.1.4/32 via 30.1.1.2
E2 172.18.1.5/32 via 30.1.1.2
E2 172.18.1.6/32 via 30.1.1.2
E2 172.18.1.7/32 via 30.1.1.2
E2 172.18.1.8/32 via 30.1.1.2
```

# Routing Information Protocol information

The following table describes the Routing Information Protocol (RIP) information commands.

Table 34 RIP information commands

| Command | Usage |
|---|---|
| **show ip rip routes** | Displays RIP routes.<br>**Command mode**: All except User EXEC |
| **show ip rip interface [***<1-255>***]** | Displays RIP interface information.<br>**Command mode**: All except User EXEC |
| **show interface ip [***<1-255>***] rip** | Displays RIP user's configuration.<br>**Command mode**: All |

## RIP Routes information

The following command displays RIP route information:

**show ip rip routes**

**Command mode:** All except User EXEC

```
3.0.0.0/8 via 30.1.1.11 metric 4
4.0.0.0/16 via 30.1.1.11 metric 16
10.0.0.0/8 via 30.1.1.2 metric 3
20.0.0.0/8 via 30.1.1.2 metric 2
```

This table contains all dynamic routes learned through RIP, including the routes that are undergoing garbage collection with metric = 16. This table does not contain directly connected routes and locally configured static routes.

## RIP user configuration

The following command displays RIP user information:

**show interface ip [***<1-255>***] rip**

**Command mode:** All

```
RIP USER CONFIGURATION :
RIP on updat 30
RIP Interface 2 : 102.1.1.1, enabled
version 2, listen enabled, supply enabled, default none
poison disabled, trigg enabled, mcast enabled, metric 1
auth none,key none
RIP Interface 3 : 103.1.1.1, enabled
version 2, listen enabled, supply enabled, default none
poison disabled, trigg enabled, mcast enabled, metric 1
```

# IP information

The following command displays Layer 3 information:

**show layer3 information**

**Command mode:** All

```
Interface information:
  1: 47.80.23.243    255.255.254.0   47.80.23.255,    vlan 1, up
Default gateway information: metric strict
  1: 47.80.22.1,      up
  2: 47.80.225.2,     up
```

The following interface and default gateway information is displayed:

- Interface number
- IP address
- IP mask
- IP broadcast address
- Operational status

# IGMP multicast group information

The following table describes the commands used to display information about IGMP groups learned by the switch.

Table 35 IGMP Multicast Group commands

| Command | Usage |
|---|---|
| **show ip igmp groups address** *<IP address>* | Displays a single IGMP multicast group by its IP address.<br>**Command mode**: All except User EXEC |
| **show ip igmp groups vlan** *<1-4094>* | Displays all IGMP multicast groups on a single VLAN.<br>**Command mode**: All except User EXEC |
| **show ip igmp groups interface** *<port number>* | Displays all IGMP multicast groups on a single port.<br>**Command mode**: All except User EXEC |
| **show ip igmp groups PortChannel** *<1-40>* | Displays all IGMP multicast groups on a single trunk group.<br>**Command mode**: All except User EXEC |
| **show ip igmp groups** | Displays information for all multicast groups.<br>**Command mode**: All except User EXEC |

# IGMP multicast router port information

The following table describes the commands used to display information about multicast routers learned through IGMP Snooping.

Table 36 IGMP Multicast Router information commands

| Command | Usage |
|---|---|
| **show ip igmp mrouter vlan** *<1-4094>* | Displays information for all multicast groups on a single VLAN.<br>**Command mode**: All except User EXEC |
| **show ip igmp mrouter information** | Displays information for all multicast groups learned by the switch.<br>**Command mode**: All except User EXEC |

# VRRP information

Virtual Router Redundancy Protocol (VRRP) support on this switch provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

The following command displays VRRP information:

**`show ip vrrp information`**

**Command mode:** All except User EXEC

```
VRRP information:
1: vrid 2, 205.178.18.210, if 1, renter, prio 100, master, server
2: vrid 1, 205.178.18.202, if 1, renter, prio 100, backup
3: vrid 3, 205.178.18.204, if 1, renter, prio 100, master, proxy
```

When virtual routers are configured, you can view the status of each virtual router using this command. VRRP information includes:

- Virtual router number
- Virtual router ID and IP address
- Interface number
- Ownership status
  - `owner` identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same.
  - `renter` identifies virtual routers which are not owned by this device
- Priority value. During the election process, the virtual router with the highest priority becomes master.
- Activity status
  - `master` identifies the elected master virtual router.
  - `backup` identifies that the virtual router is in backup mode.
  - `init` identifies that the virtual router is waiting for a startup event. Once it receives a startup event, it transitions to master if its priority is 255, (the IP address owner), or transitions to backup if it is not the IP address owner.
- Server status. The `server` state identifies virtual routers.
- Proxy status. The proxy state identifies virtual proxy routers, where the virtual router shares the same IP address as a proxy IP address. The use of virtual proxy routers enables redundant switches to share the same IP address, minimizing the number of unique IP addresses that must be configured.

# 802.1p information

The following command displays 802.1p information:

**`show qos transmit-queue information`**

**Command mode:** All

```
Current priority to COS queue information:
Priority  COSq  Weight
--------  ----  ------
    0       0      1
    1       0      1
    2       0      1
    3       0      1
    4       1      2
    5       1      2
    6       1      2
    7       1      2

Current port priority information:
Port   Priority  COSq  Weight
-----  --------  ----  ------
   1       0       0      1
   2       0       0      1
   3       0       0      1
   4       0       0      1
…
  23       0       0      1
  24       0       0      1
```

The following table describes the IEEE 802.1p priority to COS queue information.

Table 37 802.1p Priority to COS Queue information

| Field | Description |
|---|---|
| Priority | Displays the 802.1p Priority level. |
| Cosq | Displays the Class of Service queue. |
| Weight | Displays the scheduling weight of the COS queue. |

The following table describes the IEEE 802.1p port priority information.

Table 38 802.1p Port Priority information

| Field | Description |
|---|---|
| Port | Displays the port number. |
| Priority | Displays the 802.1p Priority level. |
| Cosq | Displays the Class of Service queue. |
| Weight | Displays the scheduling weight. |

# ACL information

The following table describes the commands used to display information about Access Control Lists and Groups.

Table 39 ACL information commands

| Command | Usage |
|---|---|
| **show access-control list** *<1-762>* | Displays information about the selected ACL.<br>**Command mode**: All except User EXEC |
| **show access-control group** *<1-762>* | Displays information about ACL Groups.<br>**Command mode**: All except User EXEC |
| **show access-control** | Displays information about all ACLs.<br>**Command mode**: All |

The following command displays Access Control List information:

**show access-control**

**Command mode:** All

```
Current ACL information:
------------------------
  Filter 1 profile:
   Ethernet
     - VID        : 1/0xfff
   Actions        : Set COS to 0
  Filter 2 profile:
   Ethernet
     - VID        : 1/0xfff
   Actions        : Permit
  No ACL groups configured.
```

ACL information provides configuration parameters for each Access Control List. It also shows which ACLs are included in each ACL Group.

# RMON Information

The following command displays general RMON information:

**show rmon**

**Command mode:** All

## RMON history information

The following command displays RMON history information:

**show rmon history**

**Command mode:** All

```
RMON History group configuration:

Index               IFOID              Interval  Rbnum  Gbnum
-----  -------------------------------  --------  -----  -----
    1          1.3.6.1.2.1.2.2.1.1.24        30      5      5
    2          1.3.6.1.2.1.2.2.1.1.24        30      5      5
    3          1.3.6.1.2.1.2.2.1.1.18        30      5      5
    4          1.3.6.1.2.1.2.2.1.1.19        30      5      5
    5          1.3.6.1.2.1.2.2.1.1.24      1800      5      5
```

The following table describes the RMON History Information parameters.

Table 40 RMON History Information

| Command | Usage |
|---|---|
| Index | Displays the index number that identifies each history instance. |
| IFOID | Displays the MIB Object Identifier. |
| Interval | Displays the time interval for each for each sampling bucket. |
| Rbnum | Displays the number of requested buckets, which is the number of data slots into which data is to be saved. |
| Gbnum | Displays the number of granted buckets that may hold sampled data. |

## RMON alarm information

The following command displays RMON alarm information:

**show rmon alarm**

**Command mode:** All

```
RMON Alarm group configuration:

Index  Interval  Type   rLimit    fLimit   rEvtIdx  fEvtIdx  last value
-----  --------  ----  --------  --------  -------  -------  ----------
    1        30   abs        10         0        1        0           0
    2       900   abs         0        10        0        2           0
    3       300   abs        10        20        0        0           0
    4      1800   abs        10         0        1        0           0
    5      1800   abs        10         0        1        0           0
    8      1800   abs        10         0        1        0    56344540
   10      1800   abs        10         0        1        0           0
   11      1800   abs        10         0        1        0           0
   15      1800   abs        10         0        1        0           0
   18      1800   abs        10         0        1        0           0
  100      1800   abs        10         0        1        0           0

Index               OID
-----  ------------------------------
    1        1.3.6.1.2.1.2.2.1.10.257
    2        1.3.6.1.2.1.2.2.1.11.258
    3        1.3.6.1.2.1.2.2.1.12.259
    4        1.3.6.1.2.1.2.2.1.13.260
    5        1.3.6.1.2.1.2.2.1.14.261
    8        1.3.6.1.2.1.2.2.1.10.280
   10        1.3.6.1.2.1.2.2.1.15.262
   11        1.3.6.1.2.1.2.2.1.16.263
   15        1.3.6.1.2.1.2.2.1.19.266
   18        1.3.6.1.2.1.2.2.1.10.279
  100        1.3.6.1.2.1.2.2.1.17.264
```

The following table describes the RMON Alarm Information parameters.

Table 41 RMON Alarm Information

| Command | Usage |
|---|---|
| Index | Displays the index number that identifies each alarm instance. |
| Interval | Displays the time interval over which data is sampled and compared with the rising and falling thresholds. |
| Type | Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows:<br>abs: absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.<br>delta: delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds. |
| rLimit | Displays the rising threshold for the sampled statistic. |
| fLimit | Displays the falling threshold for the sampled statistic. |
| rEvtIdx | Displays the rising alarm event index that is triggered when a rising threshold is crossed. |
| fEvtIdx | Displays the falling alarm event index that is triggered when a falling threshold is crossed. |
| Last value | Displays the last sampled value. |
| OID | Displays the MIB Object Identifier for each alarm index. |

## RMON event information

The following command displays RMON event information:

**`show rmon event`**

**Command mode:** All

```
RMON Event group configuration:

Index  Type     Last Sent                Description
-----  ----  ----------------  ---------------------------------
    1  both    0D: 0H: 1M:20S   Event_1
    2  none    0D: 0H: 0M: 0S   Event_2
    3   log    0D: 0H: 0M: 0S   Event_3
    4  trap    0D: 0H: 0M: 0S   Event_4
    5  both    0D: 0H: 0M: 0S   Log and trap event for Link Down
   10  both    0D: 0H: 0M: 0S   Log and trap event for Link Up
   11  both    0D: 0H: 0M: 0S   Send log and trap for icmpInMsg
   15  both    0D: 0H: 0M: 0S   Send log and trap for icmpInEchos
  100  both    0D: 0H: 0M: 0S   Event_100
```

The following table describes the RMON Event Information parameters.

Table 42 RMON Event Information

| Command | Usage |
|---|---|
| Index | Displays the index number that identifies each event instance. |
| Type | Displays the type of notification provided for this event, as follows: log, trap, both. |
| Last Sent | Displays the time that passed since the last switch reboot, when the most recent event was triggered. This value is cleared when the switch reboots. |
| Description | Displays a text description of the event. |

# Link status information

The following command displays link information:

**`show interface link`**

**Command mode:** All

```
------------------------------------------------------------------------
Port  Phy-Type  Speed    Duplex     Flow Ctrl      Link
----  --------  -----   --------  --TX-----RX--   ------
  1       GE     1000       any     yes    yes      down
  2       GE     1000       any     yes    yes      down
  3       GE     1000      full     yes    yes      down
  4       GE     1000      full     yes    yes      down
  5       GE     1000       any     yes    yes      down
  6       GE     1000       any     yes    yes      down
  7       GE     1000       any     yes    yes      down
  8       GE     1000      full     yes    yes       up
  9       GE     1000      full     yes    yes      down
 10       GE     1000      full     yes    yes      down
 11       GE     1000       any     yes    yes      down
 12       GE     1000       any     yes    yes      down
 13       GE     1000       any     yes    yes      down
 14       GE     1000       any     yes    yes      down
 15       GE     1000       any     yes    yes      down
 16       GE     1000       any     yes    yes      down
 17       GE     1000      full     yes    yes       up
 18       GE     1000      full     yes    yes       up
 19       GE      100      full     yes    yes       up
 20       GE      100      full     yes    yes      down
 21       GE     1000      full     yes    yes      down
 22       GE     1000       any     yes    yes      down
 23      SFP      any      full      no     no       up
 24      SFP      any      full      no     no       up
```

Use this command to display link status information about each port on a switch, including:

- Port number
- Phy-type (GE or SFP)
- Port speed (10 Mb/s, 100 Mb/s, 1000 Mb/s, or any)
- Duplex mode (half, full, or any)
- Flow control for transmit and receive (no, yes, or any)
- Link status (up or down)

# Port information

The following command displays port information:

**`show interface information`**

**Command mode:** All

```
Port Tag Media RMON PVID      NAME                 VLAN(s)
---- --- ----- ---- ---- -------------- --------------------------------
  1   n  Auto   d      1 Downlink1      1
  2   n  Auto   d      1 Downlink2      1
  3   n  Auto   d      1 Downlink3      1
  4   n  Auto   d      1 Downlink4      1
  5   n  Auto   d      1 Downlink5      1
  6   n  Auto   d      1 Downlink6      1
  7   n  Auto   d      1 Downlink7      1
  8   n  Auto   d      1 Downlink8      1
  9   n  Auto   d      1 Downlink9      1
 10   n  Auto   d      1 Downlink10     1
 11   n  Auto   d      1 Downlink11     1
 12   n  Auto   d      1 Downlink12     1
 13   n  Auto   d      1 Downlink13     1
 14   n  Auto   d      1 Downlink14     1
 15   n  Auto   d      1 Downlink15     1
 16   n  Auto   d      1 Downlink16     1
 17   n  Auto   d      1 Xconnect1      1
 18   n  Auto   d      1 Xconnect2      1
 19   n  Auto   d   4095 Mgmt           4095
 20   n  Auto   d      1 Uplink1        1
 21   n  Auto   d      1 Uplink2        1
 22   n  Auto   d      1 Uplink3        1
 23   n  Auto   d      1 Uplink4        1
 24   n  Auto   d      1 Uplink5        1
```

Port information includes:

- Port number
- Whether the port uses VLAN tagging or not (y or n)
- Media type (Auto, Copper, or Fiber)
- Whether Remote Monitoring (RMON) is enabled or disabled (e or d)
- Port VLAN ID (PVID)
- Port name
- VLAN membership

# Logical Port to GEA Port mapping

The following command displays information about GEA ports:

**show geaport**

Command mode: All

```
Logical Port  GEA Port(0-based)  GEA Unit
------------  -----------------  ---------
     1                1                0
     2                2                0
     3                4                0
     4                7                0
     5                8                0
     6               12                0
     7               13                0
     8               14                0
     9                0                0
    10                3                0
    11                5                0
    12                6                0
    13                9                0
    14               10                0
    15               11                0
    16               15                0
    17               16                0
    18               17                0
    19               18                0
    20               19                0
    21               23                0
    22               22                0
    23               21                0
    24               20                0
```

This display correlates the logical port number to the GEA unit on which each port resides.

# SFP information

The following command displays information about SFP modules:

**show sfp**

Command mode: All

```
Port   Device TX-Enable RX-Signal TX-Fault
------ ------ --------- --------- --------
SFP21  FI-SFP   **** NOT Installed ****
SFP22  FI-SFP   **** NOT Installed ****
SFP23  FI-SFP  enabled      ok      none
SFP24  FI-SFP  enabled      ok      none
```

# Uplink Failure Detection information

The following command displays Uplink Failure Detection (UFD) information:

**`show ufd`**

**Command mode:** All

```
Uplink Failure Detection 1: Enabled
LtM status: Down
Member      STG    STG State       Link Status
---------   ---    ------------    -----------
  port 24                          down
             1       DISABLED
            10       DISABLED *
            15       DISABLED *
* = STP turned off for this port.

LtD status: Auto Disabled
Member       Link Status
---------    -----------
  port  1      disabled
  port  2      disabled
  port  3      disabled
  port  4      disabled

Uplink Failure Detection 2: Disabled

Uplink Failure Detection 3: Disabled

Uplink Failure Detection 4: Disabled
```

Uplink Failure Detection (UFD) information includes:

- UFD status, either enabled or disabled
- LtM status and member ports
- Spanning Tree status for LtM ports
- LtD status and member ports

# Information dump

The following command dumps switch information:

**`show information-dump`**

**Command mode:** All

Use the dump command to dump all switch information available from this switch memory (10K or more, depending on your configuration). This data is useful for tuning and debugging switch performance.

If you want to capture dump data to a file, set the communication software on your workstation to capture session data prior to issuing the dump commands.

# Statistics commands

## Introduction

You can view switch performance statistics in the user, operator, and administrator command modes. This chapter discusses how to use the ISCLI to display switch statistics.

The following table describes general Statistics commands.

Table 43 Statistics commands

| Command | Usage |
|---|---|
| **show layer3 counters** | Displays Layer 3 Statistics.<br>**Command mode**: All |
| **show snmp-server counters** | Displays SNMP statistics.<br>**Command mode**: All |
| **show ntp counters** | Displays Network Time Protocol (NTP) Statistics.<br>You can execute the clear command option to delete all statistics.<br>**Command mode**: All |
| **clear ntp** | Clears Network Time Protocol (NTP) Statistics.<br>**Command mode**: All except User EXEC |
| **show ufd counters** | Displays Uplink Failure Detection statistics.<br>**Command mode**: All |
| **show counters** | Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.<br>**Command mode**: All |

## Port Statistics

The following table describes the Port Statistics commands. The following sections provide more detailed information and commands.

Table 44 Port Statistics commands

| Command | Usage |
|---|---|
| **show interface gigabitethernet <***port number***> dot1x counters** | Displays IEEE 802.1x statistics for the port.<br>**Command mode**: All |
| **show interface gigabitethernet** *<port number>* **bridging-counters** | Displays bridging (“dot1”) statistics for the port.<br>**Command mode**: All |
| **show interface gigabitethernet** *<port number>* **ethernet-counters** | Displays Ethernet (“dot3”) statistics for the port.<br>**Command mode**: All |
| **show interface gigabitethernet** *<port number>* **interface-counters** | Displays interface statistics for the port.<br>**Command mode**: All |
| **show interface gigabitethernet** *<port number>* **ip-counters** | Displays Internet Protocol statistics for the port.<br>**Command mode**: All |
| **show interface gigabitethernet** *<port number>* **link-counters** | Displays link statistics for the port.<br>**Command mode**: All |
| **show interface gigabitethernet** *<port number>* **rmon-counters** | Displays RMON statistics for the port.<br>**Command mode**: All |

# 802.1x statistics

Use the following command to display the 802.1x authenticator statistics of the selected port:

**show interface gigabitethernet <*port number*> dot1x counters**

**Command mode:** All

```
Authenticator Statistics:
  eapolFramesRx          = 0
  eapolFramesTx          = 0
  eapolStartFramesRx     = 0
  eapolLogoffFramesRx    = 0
  eapolRespIdFramesRx    = 0
  eapolRespFramesRx      = 0
  eapolReqIdFramesTx     = 0
  eapolReqFramesTx       = 0
  invalidEapolFramesRx   = 0
  eapLengthErrorFramesRx = 0
  lastEapolFrameVersion  = 0
  lastEapolFrameSource   = 00:00:00:00:00:00

Authenticator Diagnostics:
  authEntersConnecting                  = 0
  authEapLogoffsWhileConnecting         = 0
  authEntersAuthenticating              = 0
  authSuccessesWhileAuthenticating      = 0
  authTimeoutsWhileAuthenticating       = 0
  authFailWhileAuthenticating           = 0
  authReauthsWhileAuthenticating        = 0
  authEapStartsWhileAuthenticating      = 0
  authEapLogoffWhileAuthenticating      = 0
  authReauthsWhileAuthenticated         = 0
  authEapStartsWhileAuthenticated       = 0
  authEapLogoffWhileAuthenticated       = 0
  backendResponses                      = 0
  backendAccessChallenges               = 0
  backendOtherRequestsToSupplicant      = 0
  backendNonNakResponsesFromSupplicant = 0
  backendAuthSuccesses                  = 0
  backendAuthFails                      = 0
```

The following table describes the 802.1x authenticator diagnostics for a selected port:

Table 45 802.1x statistics for port

| Statistics | Description |
|---|---|
| Authenticator Diagnostics | |
| `authEntersConnecting` | Total number of times that the state machine transitions to the CONNECTING state from any other state. |
| `authEapLogoffsWhileConnecting` | Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message. |
| `authEntersAuthenticating` | Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAPResponse/ Identity message being received from the Supplicant. |
| `authSuccessesWhile Authenticating` | Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant. |
| `authTimeoutsWhileAuthenticating` | Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout. |

Table 45 802.1x statistics for port

| Statistics | Description |
|---|---|
| authFailWhileAuthenticating | Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure. |
| authReauthsWhileAuthenticating | Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request |
| authEapStartsWhileAuthenticating | Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant. |
| authEapLogoffWhileAuthenticating | Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant. |
| authReauthsWhileAuthenticated | Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request. |
| authEapStartsWhileAuthenticated | Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant. |
| authEapLogoffWhileAuthenticated | Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOLLogoff message being received from the Supplicant. |
| backendResponses | Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server. |
| backendAccessChallenges | Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator. |
| backendOtherRequestsToSupplicant | Total number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant. Indicates that the Authenticator chose an EAP-method. |
| backendNonNakResponsesFrom Supplicant | Total number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticators chosen EAP-method. |
| backendAuthSuccesses | Total number of times that the state machine receives an Accept message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server. |
| backendAuthFails | Total number of times that the state machine receives a Reject message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server. |

## Bridging statistics

Use the following command to display the bridging statistics of the selected port:

**show interface gigabitethernet** *<port number>* **bridging-counters**

**Command mode:** All

```
Bridging statistics for port 1:
dot1PortInFrames:                   63242584
dot1PortOutFrames:                  63277826
dot1PortInDiscards:                        0
dot1TpLearnedEntryDiscards:                0
dot1StpPortForwardTransitions:             0
```

The following table describes the bridging statistics for a selected port:

Table 46 Bridging statistics for port

| Statistics | Description |
|---|---|
| dot1PortInFrames | The number of frames that have been received by this port from its segment.<br>A frame received on the interface corresponding to this port is counted by this object, if and only if, it is for a protocol being processed by the local bridging function, including bridge management frames. |
| dot1PortOutFrames | The number of frames that have been transmitted by this port to its segment.<br>A frame transmitted on the interface corresponding to this port is counted by this object, if and only if, it is for a protocol being processed by the local bridging function, including bridge management frames. |
| dot1PortInDiscards | Count of valid frames received which were discarded (that is, filtered) by the forwarding process. |
| dot1TpLearnedEntryDiscards | The total number of Forwarding Database entries, which have been or would have been learned, but have been discarded due to a lack of space to store them in the Forwarding Database.<br>If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has adverse performance effects on the sub network).<br>If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent. |
| dot1StpPortForwardTransitions | The number of times this port has transitioned from the Learning state to the Forwarding state. |

## Ethernet statistics

Use the following command to display the ethernet statistics of the selected port:

**show interface gigabitethernet** *<port number>* **ethernet-counters**

**Command mode:** All

```
Ethernet statistics for port 1:
dot3StatsAlignmentErrors:                  0
dot3StatsFCSErrors:                        0
dot3StatsSingleCollisionFrames:            0
dot3StatsMultipleCollisionFrames:          0
dot3StatsLateCollisions:                   0
dot3StatsExcessiveCollisions:              0
dot3StatsInternalMacTransmitErrors:        0
dot3StatsFrameTooLongs:                    0
dot3StatsInternalMacReceiveErrors:         0
```

The following table describes the Ethernet statistics for a selected port:

Table 47 Ethernet statistics for port

| Statistics | Description |
|---|---|
| dot3StatsAlignmentErrors | A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check.<br>The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user).<br>Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| dot3StatsFCSErrors | A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check.<br>The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user).<br>Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| dot3StatsSingleCollisionFrames | A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.<br>A frame that is counted by an instance of this object is also counted by the corresponding instance of the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrame object. |
| dot3StatsMultipleCollisionFrames | A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.<br>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object. |
| dot3StatsLateCollisions | The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics. |
| dot3StatsExcessiveCollisions | A count of frames for which transmission on a particular interface fails due to excessive collisions. |
| dot3StatsInternalMacTransmitErrors | A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.<br>A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.<br>The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted. |

Table 47 Ethernet statistics for port

| Statistics | Description |
|---|---|
| dot3StatsFrameTooLongs | A count of frames received on a particular interface that exceeds the maximum permitted frame size.<br>The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user).<br>Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| dot3StatsInternalMacReceiveErrors | A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.<br>A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object.<br>The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted. |

## Interface statistics

Use the following command to display the interface statistics of the selected port:

**show interface gigabitethernet** *<port number>* **interface-counters**

**Command mode:** All

```
Interface statistics for port 1:
                     ifHCIn Counters       ifHCOut Counters
Octets:                  51697080313            51721056808
UcastPkts:                  65356399               65385714
BroadcastPkts:                     0                   6516
MulticastPkts:                     0                      0
Discards:                          0                      0
Errors:                            0                  21187
```

The following table describes the interface (IF) statistics for a selected port:

Table 48 Interface statistics for port

| Statistics | Description |
|---|---|
| Octets—IfHCIn | The total number of octets received on the interface, including framing characters. |
| UcastPkts—IfHCIn | The number of packets, delivered by this sublayer to a higher sublayer, which were not addressed to a multicast or broadcast address at this sublayer. |
| BroadcastPkts—IfHCIn | The number of packets, delivered by this sublayer to a higher sublayer, which were addressed to a broadcast address at this sublayer. |
| MulticastPkts—IfHCIn | The total number of packets, delivered by this sublayer. These are the packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sublayer, including those that were discarded or not sent.<br>For a MAC layer protocol, this includes both group and functional addresses. |
| Discards—IfHCIn | The number of inbound packets which were chosen to be discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. |
| Errors—IfHCIn | For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.<br>For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. |
| Octets—IfHCOut | The total number of octets transmitted out of the interface, including framing characters. |

Table 48 Interface statistics for port

| Statistics | Description |
|---|---|
| UcastPkts—IfHCOut | The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent. |
| BroadcastPkts—IfHCOut | The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sublayer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts. |
| MulticastPkts—IfHCOut | The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sublayer, including those that were discarded or not sent.<br>For a MAC layer protocol, this includes both group and functional addresses. This object is a 64-bit version of ifOutMulticastPkts. |
| Discards—IfHCOut | The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. |
| Errors—IfHCOut | For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors.<br>For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. |

## Internet Protocol (IP) statistics

Use the following command to display the interface protocol statistics of the selected port:

**show interface gigabitethernet** *<port number>* **ip-counters**

**Command mode:** All

```
GEA IP statistics for port 1:
ipInReceives   :         0
ipInHeaderError:         0
ipInDiscards   :         0
```

The following table describes the Internet Protocol (IP) statistics for a selected port:

Table 49 IP statistics for port

| Statistics | Description |
|---|---|
| ipInReceives | The total number of input datagrams received from interfaces, including those received in error. |
| ipInHeaderError | The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). |
| ipInDiscards | The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly. |

## Link statistics

Use the following command to display the link statistics of the selected port:

**show interface gigabitethernet** *<port number>* **link-counters**

**Command mode:** All

```
Link statistics for port 1:
linkStateChange:              2
```

The following table describes the link statistics for a selected port:

Table 50 Link statistics for port

| Statistic | Description |
|---|---|
| linkStateChange | The total number of link state changes. |

## Port RMON statistics

Use the following command to display the RMON statistics of the selected port:

**show interface gigabitethernet** *<port number>* **rmon-counters**

**Command mode:** All

```
RMON statistics for port 2:
etherStatsDropEvents:                        NA
etherStatsOctets:                             0
etherStatsPkts:                               0
etherStatsBroadcastPkts:                      0
etherStatsMulticastPkts:                      0
etherStatsCRCAlignErrors:                     0
etherStatsUndersizePkts:                      0
etherStatsOversizePkts:                       0
etherStatsFragments:                          0
etherStatsJabbers:                            0
etherStatsCollisions:                         0
etherStatsPkts64Octets:                       0
etherStatsPkts65to127Octets:                  0
etherStatsPkts128to255Octets:                 0
etherStatsPkts256to511Octets:                 0
etherStatsPkts64Octets:                       0
etherStatsPkts1024to1518Octets:               0
```

The following table describes the Remote Monitoring (RMON) statistics of the selected port:

Table 51 RMON statistics

| Statistic | Description |
|---|---|
| etherStatsDropEvents | The total number of packets received that were dropped because of system resource constraints. |
| etherStatsOctets | The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). |
| etherStatsPkts | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| etherStatsBroadcastPkts | The total number of good packets received that were directed to the broadcast address. |
| etherStatsMulticastPkts | The total number of good packets received that were directed to a multicast address. |
| etherStatsCRCAlignErrors | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| etherStatsUndersizePkts | The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. |

Table 51 RMON statistics

| Statistic | Description |
|---|---|
| etherStatsOversizePkts | The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed. |
| etherStatsFragments | The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| etherStatsJabbers | The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. |
| etherStatsCollisions | The best estimate of the total number of collisions on this Ethernet segment. |
| etherStatsPkts64 Octets | The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets). |
| etherStatsPkts65to127 Octets | The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets). |
| etherStatsPkts128to255 Octets | The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets). |
| etherStatsPkts256to511 Octets | The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCSoctets). |
| etherStatsPkts512to1023 Octets | The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets). |
| etherStatsPkts1024to1518 Octets | The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets). |

# Layer 2 statistics

The following table describes the Layer 2 statistics commands. The following sections provide more detailed information and commands.

Table 52 Layer 2 Statistics commands

| Command | Usage |
|---|---|
| **show mac-address-table counters** | Displays the Forwarding Database statistics.<br>**Command mode**: All |
| **show interface gigabitethernet <***port number***> lacp counters** | Displays Link Aggregation Control Protocol (LACP) statistics.<br>**Command mode**: All |

## FDB statistics

Use the following command to display statistics regarding the use of the forwarding database:

**show mac-address-table counters**

**Command mode:** All

```
FDB statistics:
 current:            91   hiwat:               91
```

These commands enable you to display statistics regarding the use of the forwarding database, including the number of current entries and the maximum number of entries ever recorded.

The following table describes the Forwarding Database (FDB) statistics:

Table 53 Forwarding Database statistics

| Statistic | Description |
|---|---|
| current | Current number of entries in the Forwarding Database. |
| hiwat | Highest number of entries recorded at any given time in the Forwarding Database. |

## LACP statistics

Use the following command to display Link Aggregation Control Protocol (LACP) statistics:

**show interface gigabitethernet <***port number***> lacp counters**

Command mode: All

```
Valid LACPDUs received         - 0
Valid Marker PDUs received     - 0
Valid Marker Rsp PDUs received - 0
Unknown version/TLV type       - 0
Illegal subtype received       - 0
LACPDUs transmitted            - 0
Marker PDUs transmitted        - 0
Marker Rsp PDUs transmitted    - 0
```

# Layer 3 statistics

The following table describes basic Layer 3 statistics commands. The following sections provide more detailed information and commands. Layer 3 functionality is limited in this release.

Table 54 Layer 3 Statistics commands

| Command | Usage |
|---|---|
| **show ip counters** | Displays IP statistics.<br>**Command mode**: All except UserEXEC |
| **clear ip counters** | Clears IP statistics. Use this command with caution as it deletes all the IP statistics.<br>**Command mode**: All except UserEXEC |
| **show ip route counters** | Displays route statistics.<br>**Command mode**: All except User EXEC |
| **show ip arp counters** | Displays Address Resolution Protocol (ARP) statistics.<br>**Command mode**: All except UserEXEC |
| **show ip dns counters** | Displays Domain Name System (DNS) statistics.<br>**Command mode**: All except UserEXEC |
| **show ip icmp counters** | Displays ICMP statistics.<br>**Command mode**: All except UserEXEC |
| **show ip tcp counters** | Displays Transmission Control Protocol (TCP) statistics.<br>**Command mode**: All except UserEXEC |
| **show ip udp counters** | Displays User Datagram Protocol (UDP) statistics. Add the argument, clear, to clear UDP statistics.<br>**Command mode**: All except UserEXEC |
| **show ip igmp counters** | Displays IGMP statistics.<br>**Command mode**: All except UserEXEC |
| **clear ip igmp [***<1-4094>***] counters** | Clears all IGMP statistics for the selected VLANs.<br>**Command mode**: All except UserEXEC |
| **show ip ospf counters** | Displays OSPF statistics.<br>**Command mode**: All except UserEXEC |
| **show ip vrrp counters** | When virtual routers are configured, you can display the following<br>• Advertisements received (vrrpInAdvers)<br>• Advertisements transmitted (vrrpOutAdvers)<br>• Advertisements received, but ignored (vrrpBadAdvers)<br>**Command mode**: All except UserEXEC |
| **show ip rip counters** | Displays Routing Information Protocol (RIP) statistics.<br>**Command mode**: All except UserEXEC |
| **show ip gea** | Displays GEA statistics.<br>**Command mode**: All except UserEXEC |
| **show layer3 counters** | Displays all Layer 3 statistics.<br>**Command mode**: All |

# IP statistics

The following command displays IP statistics:

**show ip counters**

**Command mode:** All except User EXEC

```
IP statistics:
ipInReceives: 36475             ipInHdrErrors: 0
ipInAddrErrors: 905
ipInUnknownProtos: 0            ipInDiscards: 0
ipInDelivers: 4103              ipOutRequests: 30974
ipOutDiscards: 0
ipDefaultTTL: 255
```

The following table describes the IP statistics:

Table 55 IP statistics

| Statistics | Description |
|---|---|
| ipInReceives | The total number of input datagrams received from interfaces, including those received in error. |
| ipInHdrErrors | The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on. |
| ipInAddrErrors | The number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this switch. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E).<br>For entities which are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |
| ipInUnknownProtos | The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. |
| ipInDiscards | The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space).<br>This counter does not include any datagrams discarded while awaiting re-assembly. |
| ipInDelivers | The total number of input datagrams successfully delivered to IP user-protocols (including ICMP). |
| ipOutRequests | The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission.<br>This counter does not include any datagrams counted in ipForwDatagrams. |
| ipOutDiscards | The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space).<br>This counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion. |
| ipDefaultTTL | The default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this switch, whenever a TTL value is not supplied by the transport layer protocol. |

## Route statistics

The following command displays route statistics:

**show ip route counters**

**Command mode:** All except User EXEC

```
Route statistics:
ipRoutesCur:               7  ipRoutesHighWater:         7
ipRoutesMax:             512
```

The following table describes the Route statistics:

Table 56 Route statistics

| Statistics | Description |
|---|---|
| ipRoutesCur | The total number of outstanding routes in the route table. |
| ipRoutesMax | The maximum number of supported routes. |
| ipRoutesHighWater | The highest number of routes ever recorded in the route table. |

## ARP statistics

The following command displays Address Resolution Protocol statistics.

**show ip arp counters**

**Command mode:** All except User EXEC

```
ARP statistics:
arpEntriesCur:             2  arpEntriesHighWater:          4
```

The following table describes the Address Resolution Protocol (ARP) statistics:

Table 57 ARP statistics

| Statistic | Description |
|---|---|
| arpEntriesCur | The total number of outstanding ARP entries in the ARP table. |
| arpEntriesHighWater | The highest number of ARP entries ever recorded in the ARP table. |

## DNS statistics

**show ip dns counters**

**Command mode:** All except User EXEC

```
DNS statistics:
dnsInRequests:             0  dnsOutRequests:            0
dnsBadRequests:            0
```

The following table describes the Domain Name System (DNS) statistics:

Table 58 DNS statistics

| Statistic | Description |
|---|---|
| dnsInRequests | The total number of DNS request packets that have been received. |
| dnsOutRequests | The total number of DNS response packets that have been transmitted. |
| dnsBadRequests | The total number of DNS request packets received that were dropped. |

# ICMP statistics

The following command displays ICMP statistics:

**show ip icmp counters**

**Command mode:** All except User EXEC

```
ICMP statistics:
icmpInMsgs:              245802   icmpInErrors:               1393
icmpInDestUnreachs:          41   icmpInTimeExcds:               0
icmpInParmProbs:              0   icmpInSrcQuenchs:              0
icmpInRedirects:              0   icmpInEchos:                  18
icmpInEchoReps:          244350   icmpInTimestamps:              0
icmpInTimestampReps:          0   icmpInAddrMasks:               0
icmpInAddrMaskReps:           0   icmpOutMsgs:              253810
icmpOutErrors:                0   icmpOutDestUnreachs:          15
icmpOutTimeExcds:             0   icmpOutParmProbs:              0
icmpOutSrcQuenchs:            0   icmpOutRedirects:              0
icmpOutEchos:            253777   icmpOutEchoReps:              18
icmpOutTimestamps:            0   icmpOutTimestampReps:          0
icmpOutAddrMasks:             0   icmpOutAddrMaskReps:           0
```

The following table describes the Internet Control Messaging Protocol (ICMP) statistics:

Table 59 ICMP statistics

| Statistics | Description |
|---|---|
| icmpInMsgs | The total number of ICMP messages which the switch received. Note that this counter includes all those counted by icmpInErrors. |
| icmpInErrors | The number of ICMP messages which the switch received but determined as having ICMP specific errors (for example bad ICMP checksums and bad length). |
| icmpInDestUnreachs | The number of ICMP Destination Unreachable messages received. |
| icmpInTimeExcds | The number of ICMP Time Exceeded messages received. |
| icmpInParmProbs | The number of ICMP Parameter Problem messages received. |
| icmpInSrcQuenchs | The number of ICMP Source Quench (buffer almost full, stop sending data) messages received. |
| icmpInRedirects | The number of ICMP Redirect messages received. |
| icmpInEchos | The number of ICMP Echo (request) messages received. |
| icmpInEchoReps | The number of ICMP Echo Reply messages received. |
| icmpInTimestamps | The number of ICMP Timestamp (request) messages received. |
| icmpInTimestampReps | The number of ICMP Timestamp Reply messages received. |
| icmpInAddrMasks | The number of ICMP Address Mask Request messages received. |
| icmpInAddrMaskReps | The number of ICMP Address Mask Reply messages received. |
| icmpOutMsgs | The total number of ICMP messages which this switch attempted to send. Note that this counter includes all those counted by icmpOutErrors. |
| icmpOutErrors | The number of ICMP messages that this switch did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value. |
| icmpOutDestUnreachs | The number of ICMP Destination Unreachable messages sent. |
| icmpOutTimeExcds | The number of ICMP Time Exceeded messages sent. |
| icmpOutParmProbs | The number of ICMP Parameter Problem messages sent. |
| icmpOutSrcQuenchs | The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent. |
| icmpOutRedirects | The number of ICMP Redirect messages sent. |
| icmpOutEchos | The number of ICMP Echo (request) messages sent. |
| icmpOutEchoReps | The number of ICMP Echo Reply messages sent. |
| icmpOutTimestamps | The number of ICMP Timestamp (request) messages sent. |
| icmpOutTimestampReps | The number of ICMP Timestamp Reply messages sent. |
| icmpOutAddrMasks | The number of ICMP Address Mask Request messages sent. |
| icmpOutAddrMaskReps | The number of ICMP Address Mask Reply messages sent. |

# TCP statistics

The following command displays TCP statistics:

**show ip tcp counters**

**Command mode:** All except User EXEC

```
TCP statistics:
tcpRtoAlgorithm:          4   tcpRtoMin:               0
tcpRtoMax:           240000   tcpMaxConn:           2048
tcpActiveOpens:      252214   tcpPassiveOpens:         7
tcpAttemptFails:        528   tcpEstabResets:          4
tcpInSegs:           756401   tcpOutSegs:         756655
tcpRetransSegs:           0   tcpInErrs:               0
tcpCurBuff:               0   tcpCurConn:              3
tcpOutRsts:             417
```

The following table describes the Transmission Control Protocol (TCP) statistics:

Table 60 TCP statistics

| Statistics | Description |
|---|---|
| tcpRtoAlgorithm | The algorithm used to determine the timeout value used for retransmitting unacknowledged octets. |
| tcpRtoMin | The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in Request For Comments (RFC) 793. |
| tcpRtoMax | The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793. |
| tcpMaxConn | The limit on the total number of TCP connections the switch can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1. |
| tcpActiveOpens | The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state. |
| tcpPassiveOpens | The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state. |
| tcpAttemptFails | The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state. |
| tcpEstabResets | The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE- WAIT state. |
| tcpInSegs | The total number of segments received, including those received in error. This count includes segments received on currently established connections. |
| tcpOutSegs | The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets. |
| tcpRetransSegs | The total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets. |
| tcpInErrs | The total number of segments received in error (for example, bad TCP checksums). |
| tcpCurBuff | The total number of outstanding memory allocations from heap by TCP protocol stack. |
| tcpCurConn | The total number of outstanding TCP sessions that are currently opened. |
| tcpOutRsts | The number of TCP segments sent containing the reset (RST) flag. |

## UDP statistics

The following command displays UDP statistics:

**show ip udp counters**

**Command mode:** All except User EXEC

```
UDP statistics:
udpInDatagrams:         54   udpOutDatagrams:         43
udpInErrors:             0   udpNoPorts:         1578077
```

The following table describes the User Datagram Protocol (UDP) statistics:

Table 61 UDP statistics

| Statistics | Description |
|---|---|
| udpInDatagrams | The total number of UDP datagrams delivered to the switch. |
| udpOutDatagrams | The total number of UDP datagrams sent from this switch. |
| udpInErrors | The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port. |
| udpNoPorts | The total number of received UDP datagrams for which there was no application at the destination port. |

## IGMP Multicast Group statistics

The following command displays statistics about the use of the IGMP Multicast Groups:

**show ip igmp counters**

**Command mode:** All except User EXEC

```
------------------------------------------------------------
IGMP Snoop vlan 1 statistics:
------------------------------------------------------------
rxIgmpValidPkts:         0    rxIgmpInvalidPkts:            0
rxIgmpGenQueries:        0    rxIgmpGrpSpecificQueries:     0
rxIgmpLeaves:            0    rxIgmpReports:                0
txIgmpReports:           0    txIgmpGrpSpecificQueries:     0
txIgmpLeaves:            0
```

These commands enable you to display statistics regarding the use of the IGMP Multicast Groups.

The following table describes the IGMP statistics:

Table 62 IGMP statistics

| Statistic | Description |
|---|---|
| rxIgmpValidPkts | Total number of valid IGMP packets received |
| rxIgmpInvalidPkts | Total number of invalid packets received |
| rxIgmpGenQueries | Total number of General Membership Query packets received |
| rxIgmpGrpSpecificQueries | Total number of Membership Query packets received from specific groups |
| rxIgmpLeaves | Total number of Leave requests received |
| rxIgmpReports | Total number of Membership Reports received |
| txIgmpReports | Total number of Membership reports transmitted |
| txIgmpGrpSpecificQueries | Total number of Membership Query packets transmitted to specific groups |
| txIgmpLeaves | Total number of Leave messages transmitted |

# OSPF statistics

The following table describes OSPF statistics commands.

Table 63 OSPF Statistics commands

| Command | Usage |
|---|---|
| **show ip ospf counters** | Displays OSPF global statistics.<br>**Command mode**: All except UserEXEC |
| **show ip ospf area <***0-2***> counters** | Displays area index statistics.<br>**Command mode**: All except UserEXEC |
| **show ip ospf interface <***1-255***> counters** | Displays interface statistics.<br>**Command mode**: All except UserEXEC |

# OSPF global statistics

The following command displays OSPF global statistics:

**show ip ospf counters**

**Command mode:** All except User EXEC

```
OSPF stats
----------
Rx/Tx Stats:                Rx              Tx
                          --------        --------
  Pkts                         0               0
  hello                       23             518
  database                     4              12
  ls requests                  3               1
  ls acks                      7               7
  ls updates                   9               7

Nbr change stats:                         Intf change Stats:
  hello                          2              up   4
  start                          0              down 2
  n2way                          2              loop 0
  adjoint ok                     2              unloop 0
  negotiation done               2              wait timer 2
  exchange done                  2              backup 0
  bad requests                   0              nbr change 5
  bad sequence                   0
  loading done                   2
  n1way                          0
  rst_ad                         0
  down                           1
Timers kickoff
  hello                        514
  retransmit                  1028
  lsa lock                       0
  lsa ack                        0
  dbage                          0
  summary                        0
  ase export                     0
```

The following table describes the OSPF global statistics:

Table 64 OSPF global statistics

| Statistic | Description |
|---|---|
| **Rx Tx stats:** | |
| Rx Pkts | The sum total of all OSPF packets received on all OSPF areas and interfaces. |
| Tx Pkts | The sum total of all OSPF packets transmitted on all OSPF areas and interfaces. |
| Rx Hello | The sum total of all Hello packets received on all OSPF areas and interfaces. |

Table 64 OSPF global statistics

| Statistic | Description |
|---|---|
| Tx Hello | The sum total of all Hello packets transmitted on all OSPF areas and interfaces. |
| Rx Database | The sum total of all Database Description packets received on all OSPF areas and interfaces. |
| Tx Database | The sum total of all Database Description packets transmitted on all OSPF areas and interfaces. |
| Rx ls Requests | The sum total of all Link State Request packets received on all OSPF areas and interfaces. |
| Tx ls Requests | The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces. |
| Rx ls Acks | The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces. |
| Tx ls Acks | The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces. |
| Rx ls Updates | The sum total of all Link State Update packets received on all OSPF areas and interfaces. |
| Tx ls Updates | The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces. |
| **Nbr change stats:** | |
| hello | The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces. |
| Start | The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds) across all OSPF areas and interfaces. |
| n2way | The sum total number of bidirectional communication establishment between this router and other neighboring routers. |
| adjoint ok | The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces. |
| negotiation done | The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces. |
| exchange done | The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces. |
| bad requests | The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas. |
| bad sequence | The sum total number of Database Description packets which have been received that either:<br>• Has an unexpected DD sequence number<br>• Unexpectedly has the init bit set<br>• Has an options field differing from the last Options field received in a Database Description packet.<br>Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces. |
| loading done | The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces. |
| n1way | The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas. |
| rst_ad | The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces. |

Table 64 OSPF global statistics

| Statistic | Description |
|---|---|
| down | The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation) across all OSPF areas and interfaces. |
| **Intf Change Stats:** | |
| up | The sum total number of interfaces up in all OSPF areas. |
| down | The sum total number of interfaces down in all OSPF areas. |
| loop | The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces. |
| unloop | The sum total number of interfaces, connected to the attached network in all OSPF areas. |
| wait timer | The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces. |
| backup | The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces. |
| nbr change | The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas. |
| **Timers Kickoff:** | |
| hello | The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OPSF areas and interfaces. |
| retransmit | The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces. |
| lsa lock | The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces. |
| lsa ack | The sum total number of times the LSA Ack timer has been fired across all OSPF areas and interfaces. |
| dbage | The total number of times the data base age (Dbage) has been fired. |
| summary | The total number of times the Summary timer has been fired. |
| ase export | The total number of times the Autonomous System Export (ASE) timer has been fired. |

# VRRP statistics

Virtual Router Redundancy Protocol (VRRP) support on this switch provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device.

One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

When virtual routers are configured, you can display the following protocol statistics for VRRP:

- Advertisements received (`vrrpInAdvers`)
- Advertisements transmitted (`vrrpOutAdvers`)
- Advertisements received, but ignored (`vrrpBadAdvers`)

The following command displays statistics for the VRRP LAN:

**`show ip vrrp counters`**

**Command mode:** All except User EXEC

```
>> Layer 3 Statistics# vrrp
VRRP statistics:
vrrpInAdvers:               0   vrrpBadAdvers:            0
vrrpOutAdvers:              0
vrrpBadVersion:             0   vrrpBadVrid:              0
vrrpBadAddress:             0   vrrpBadData:              0
vrrpBadPassword:            0   vrrpBadInterval:          0
```

The following table describes the VRRP statistics.

Table 65 VRRP statistics

| Field | Description |
|---|---|
| `vrrpInAdvers` | The total number of VRRP advertisements that have been received. |
| `vrrpOutAdvers` | The total number of VRRP advertisements that have been sent. |
| `vrrpBadVersion` | The total number of VRRP advertisements that had a bad version number. |
| `vrrpBadAddress` | The total number of VRRP advertisements that had a bad address. |
| `vrrpBadPassword` | The total number of VRRP advertisements that had a bad password. |
| `vrrpBadAdvers` | The total number of VRRP advertisements received that were dropped. |
| `vrrpBadVrid` | The total number of VRRP advertisements that had a bad virtual router ID. |
| `vrrpBadData` | The total number of VRRP advertisements that had bad data. |
| `vrrpBadInterval` | The total number of VRRP advertisements that had a bad interval. |

# RIP statistics

The following command displays RIP statistics:

**`show ip rip counters`**

**Command mode:** All except User EXEC

```
RIP ALL STATS INFORMATION:
        RIP packets received = 12
        RIP packets sent = 75
        RIP request received = 0
        RIP response received = 12
        RIP request sent = 3
        RIP response sent = 72
        RIP route timeout = 0
        RIP bad size packet received = 0
        RIP bad version received = 0
        RIP bad zeros received = 0
        RIP bad src port received = 0
        RIP bad src IP received = 0
        RIP packets from self received = 0
```

The following table describes the basic Routing Information Protocol (RIP) statistics :

Table 66 RIP Statistics

| Statistics | Description |
|---|---|
| RIP packets received | The total number of RIP packets received. |
| RIP packets sent | The total number of RIP packets transmitted. |
| RIP request received | The total number of RIP requests received. |
| RIP response received | The total number of RIP response received. |
| RIP request sent | The total number of RIP requests transmitted. |
| RIP response sent | The total number of RIP responses transmitted. |
| RIP route timeout | The total number of RIP route timeouts. |
| RIP bad size packet received | The total number of bad size RIP packets received. |
| RIP bad version received | The total number of RIP bad versions received. |
| RIP bad zeros received | The total number of RIP bad zeros (RIPv1 packets with non-zero unused fields) received. |
| RIP bad source port received | The total number of RIP bad source port received. |
| RIP bad source IP received | The total number of RIP bad source IP received. |
| RIP packets from self received | The total number of RIP packets from self received. |

# GEA Layer 3 statistics

The following table describes the Layer 3 GEA statistics commands.

Table 67 Layer 3 GEA statistics commands

| Command | Usage |
|---|---|
| **show ip gea bucket <***IP address***>** | Displays GEA statistics for a specific IP address.<br>**Command mode**: All except User EXEC |
| **show ip gea** | Displays all GEA statistics.<br>**Command mode**: All except User EXEC |

# GEA Layer 3 statistics

The following command displays GEA statistics:

**show ip gea**

**Command mode:** All except User EXEC

```
GEA L3 statistics:
         Max L3 table size                : 2048
         Number of L3 entries used        : 0

         Max LPM table size               : 256
         Number of LPM entries used       : 0
```

# Management Processor statistics

The following table describes the MP-specific Statistics commands. The following sections provide more detailed information and commands.

Table 68 MP-specific Statistics commands

| Command | Usage |
|---|---|
| **show mp packet** | Displays packet statistics, to check for leads and load.<br>**Command mode**: All |
| **show mp tcp-block** | Displays all Transmission Control Protocol (TCP) control blocks (TCB) that are in use.<br>**Command mode**: All |
| **show mp udp-block** | Displays all User Datagram Protocol (UDP) control blocks (UCB) that are in use.<br>**Command mode**: All |
| **show mp cpu** | Displays CPU utilization for periods of up to 1, 4, and 64 seconds.<br>**Command mode**: All |

## Packet statistics

The following command displays packet statistics:

**show mp packet**

**Command mode:** All

```
Packet counts:
 allocs:          36692     frees:                       36692
 mediums:             0     mediums hi-watermark:            3
 jumbos:              0     jumbos hi-watermark:             0
 smalls:              0     smalls hi-watermark:             2
 failures:            0
```

The following table describes the packet statistics.

Table 69 MP specific packet statistics

| Description | Example statistic |
|---|---|
| allocs | Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack. |
| frees | Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack. |
| mediums | Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| mediums hi-watermark | The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| jumbos | Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| jumbos hi-watermark | The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| smalls | Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| smalls hi-watermark | The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| failures | Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack. |

## TCP statistics

The following command displays TCP statistics:

**show mp tcp-block**

**Command mode:** All

```
All TCP allocated control blocks:
10ad41e8:  0.0.0.0             0 <=> 0.0.0.0            80  listen
10ad5790:  47.81.27.5       1171 <=> 47.80.23.243       23  established
```

The following table describes the Transmission Control Protocol (TCP) control block (TCB) statistics shown in this example:

Table 70 TCP statistics

| Description | Example statistic |
|---|---|
| Memory | 10ad41e8/10ad5790 |
| Destination IP address | 0.0.0.0/47.81.27.5 |
| Destination port | 0/1171 |
| Source IP | 0.0.0.0/47.80.23.243 |
| Source port | 80/23 |
| State | listen/established |

## UDP statistics

The following command displays UDP statistics:

**show mp udp-block**

**Command mode:** All

```
All UDP allocated control blocks:
  161:  listen
```

The following table describes the User Datagram Protocol (UDP) control block (UCB) statistics shown in this example:

Table 71 UDP statistics

| Description | Example Statistic |
|---|---|
| Control block | 161 |
| State | listen |

## CPU statistics

The following command displays the CPU utilization statistics:

**show mp cpu**

**Command mode:** All

```
CPU utilization:
cpuUtil1Second:            8%
cpuUtil4Seconds:           9%
cpuUtil64Seconds:          8%
```

The following table describes the management port CPU utilization statistics:

Table 72 CPU statistics

| Statistics | Description |
|---|---|
| cpuUtil1Second | The utilization of MP CPU over 1 second. This is shown as a percentage. |
| cpuUtil4Seconds | The utilization of MP CPU over 4 seconds. This is shown as a percentage. |
| cpuUtil64Seconds | The utilization of MP CPU over 64 seconds. This is shown as a percentage. |

# ACL statistics

The following command displays the statistics for Access Control Lists (ACLs):

**show access-control counters**

**Command mode:** All

```
Hits for ACL 1: 26057515
Hits for ACL 2: 26057497
```

# SNMP statistics

The following command displays SNMP statistics:

**show snmp-server counters**

**Command mode:** All

```
SNMP statistics:
snmpInPkts:                  54   snmpInBadVersions:              0
snmpInBadC'tyNames:           0   snmpInBadC'tyUses:              0
snmpInASNParseErrs:           0   snmpEnableAuthTraps:            0
snmpOutPkts:                 54   snmpInBadTypes:                 0
snmpInTooBigs:                0   snmpInNoSuchNames:              0
snmpInBadValues:              0   snmpInReadOnlys:                0
snmpInGenErrs:                0   snmpInTotalReqVars:           105
snmpInTotalSetVars:           0   snmpInGetRequests:              2
snmpInGetNexts:              52   snmpInSetRequests:              0
snmpInGetResponses:           0   snmpInTraps:                    0
snmpOutTooBigs:               0   snmpOutNoSuchNames:             2
snmpOutBadValues:             0   snmpOutReadOnlys:               0
snmpOutGenErrs:               0   snmpOutGetRequests:             0
snmpOutGetNexts:              0   snmpOutSetRequests:             0
snmpOutGetResponses:         54   snmpOutTraps:                   0
snmpSilentDrops:              0   snmpProxyDrops:                 0
```

The following table describes the Simple Network Management Protocol (SNMP) statistics:

Table 73 SNMP statistics

| Statistics | Description |
|---|---|
| snmpInPkts | The total number of messages delivered to the SNMP entity from the transport service. |
| snmpInBadVersions | The total number of SNMP messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version. |
| snmpInBadC'tyNames | The total number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to the switch. |
| snmpInBadC'tyUses | The total number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation which was not allowed by the SNMP community named in the message. |
| snmpInASNParseErrs | The total number of ASN.1 (Abstract Syntax Notation One) or BER (Basic Encoding Rules), errors encountered by the SNMP protocol entity when decoding SNMP messages received.<br>The Open Systems Interconnection (OSI) method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209).<br>ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences.<br>BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets. |
| snmpEnableAuthTraps | An object to enable or disable the authentication traps generated by this switch. |
| snmpOutPkts | The total number of SNMP messages which were passed from the SNMP protocol entity to the transport service. |
| snmpInBadTypes | The total number of SNMP messages which failed ASN.1 parsing. |

Table 73 SNMP statistics

| Statistics | Description |
|---|---|
| snmpInTooBigs | The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is too big. |
| snmpInNoSuchNames | The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName. |
| snmpInBadValues | The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is badValue. |
| snmpInReadOnlys | The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is read-only.<br>It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value read-only in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP. |
| snmpInGenErrs | The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr. |
| snmpInTotalReqVars | The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs). |
| snmpInTotalSetVars | The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs). |
| snmpInGetRequests | The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity. |
| snmpInGetNexts | The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity. |
| snmpInSetRequests | The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity. |
| snmpInGetResponses | The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity. |
| snmpInTraps | The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity. |
| snmpOutTooBigs | The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is too big. |
| snmpOutNoSuchNames | The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is noSuchName. |
| snmpOutBadValues | The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is badValue. |
| snmpOutReadOnlys | Not in use. |
| snmpOutGenErrs | The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is genErr. |
| snmpOutGetRequests | The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity. |
| snmpOutGetNexts | The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity. |
| snmpOutSetRequests | The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity. |
| snmpOutGetResponses | The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity. |
| snmpOutTraps | The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity. |

Table 73 SNMP statistics

| Statistics | Description |
|---|---|
| snmpSilentDrops | The total number of GetRequest-PDUs, GetNextRequest-PDUs,GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was too large. |
| snmpProxyDrops | The total number of GetRequest-PDUs, GetNextRequest-PDUs,GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner (other than a time-out) such that no Response-PDU could be returned. |

# NTP statistics

The following command displays NTP statistics:

**show ntp counters**

**Command mode:** All

```
NTP statistics:
        Primary Server:
                Requests Sent:              17
                Responses Received:         17
                Updates:                    1
        Secondary Server:
                Requests Sent:              0
                Responses Received:         0
                Updates:                    0
        Last update based on response from primary server.
        Last update time: 18:04:16 Tue Mar 13, 2006
        Current system time: 18:55:49 Tue Mar 13, 2006
```

The switch uses NTP (Network Timing Protocol) version 3 to synchronize the switch's internal clock with an atomic time-calibrated NTP server. With NTP enabled, the switch can accurately update its internal clock to be consistent with other devices on the network and generates accurate syslogs.

The following table describes the NTP statistics:

Table 74 NTP statistics

| Statistics | Description |
|---|---|
| Primary Server | Requests Sent: The total number of NTP requests the switch sent to the primary NTP server to synchronize time.<br>Responses Received: The total number of NTP responses received from the primary NTP server.<br>Updates: The total number of times the switch updated its time based on the NTP responses received from the primary NTP server. |
| Secondary Server | Requests Sent: The total number of NTP requests the switch sent to the secondary NTP server to synchronize time.<br>Responses Received: The total number of NTP responses received from the secondary NTP server.<br>Updates: The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server. |
| Last update based on response from primary server | Last update of time on the switch based on either primary or secondary NTP response received. |
| Last update time | The time stamp showing the time when the switch was last updated. |
| Current system time | The switch system time when the command `show ntp counters` was issued. |

# Uplink Failure Detection statistics

The following command allows you to display Uplink Failure Detection (UFD) statistics.

**show ufd counters**

**Command mode:** All

```
Uplink Failure Detection statistics:
FDP number: 1
Number of times LtM link failure: 1
Number of times LtM link in Blocking State: 0
Number of times LtD got auto disabled: 1
FDP number: 2
Number of times LtM link failure: 1
Number of times LtM link in Blocking State: 0
Number of times LtD got auto disabled: 1
FDP number: 3
Number of times LtM link failure: 1
Number of times LtM link in Blocking State: 0
Number of times LtD got auto disabled: 1
FDP number: 4
Number of times LtM link failure: 1
Number of times LtM link in Blocking State: 0
Number of times LtD got auto disabled: 1
```

The following table describes the Uplink Failure Detection (UFD) statistics:

Table 75 Uplink Failure Detection statistics

| Statistic | Description |
|---|---|
| Number of times LtM link failure | The total numbers of times that link failures were detected on the uplink ports in the Link to Monitor group. |
| Number of times LtM link in Blocking State | The total number of times that Spanning Tree Blocking state was detected on the uplink ports in the Link to Monitor group. |
| Number of times LtD got auto disabled | The total numbers of times that downlink ports in the Link to Disable group were automatically disabled because of a failure in the Link to Monitor group. |

# Statistics dump

The following command dumps the switch statistics:

**show counters**

Use the dump command to dump all switch statistics available (40K or more, depending on your configuration). This data can be used to tune or debug switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

# Configuration Commands

## Introduction

The Configuration commands are available only from an administrator login. They include commands for configuring every aspect of the switch. Changes can be saved to non-volatile memory (NVRAM).

The following table describes the basic Configuration commands. The following sections provide more detailed information and commands.

Table 76 Configuration commands

| Command | Usage |
|---|---|
| **show running-config** | Dumps current configuration to a script file.<br>**Command mode**: All except User EXEC |
| **copy running-config {ftp\|tftp}** | Backs up current configuration to FTP/TFTP server.<br>**Command mode**: All except User EXEC |
| **copy {ftp\|tftp} running-config** | Restores current configuration from FTP/TFTP server.<br>**Command mode**: All except User EXEC |

## Viewing and saving changes

As you use the configuration commands to set switch parameters, the changes you make take effect immediately. You do not need to apply configuration changes when you use the ISCLI. Any changes are lost the next time the switch boots unless the changes are explicitly saved.

## Saving the configuration

You must save configuration changes to flash memory, so the switch reloads the setting when you reset the switch.

IMPORTANT: If you do not save the changes, they are lost the next time the system is reloaded.

To save the new configuration, enter the following command at any prompt:

```
Switch# copy running-config startup-config
```

When you save configuration changes, the changes are saved to the active configuration block.

For instructions about selecting the configuration to run at the next system reload, see the “Selecting a configuration block” section in the “Boot Options” chapter.

# System configuration

These commands allow you to configure switch management parameters such as user and administrator privilege mode passwords, browser-based management settings, and management access list.

The following table describes the System Configuration commands.

Table 77 System Configuration commands

| Command | Usage |
|---|---|
| **system date** *<yyyy> <mm> <dd>* | Prompts the user for the system date.<br>**Command mode**: Global configuration |
| **system time** *<hh>:<mm>:<ss>* | Configures the system time using a 24-hour clock format.<br>**Command mode**: Global configuration |
| **system timezone** | Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.<br>**Command mode**: Global configuration |
| **system daylight** | Disables or enables daylight saving time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. By default, this option is disabled.<br>**Command mode**: Global configuration |
| **system idle** *<1-60>* | Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 5 minutes.<br>This setting affects both the console port and Telnet port.<br>**Command mode**: Global configuration |
| **[no] system notice** *<1-1024 characters multi-line> <'-' to end>* | Displays login notice immediately before the "Enter password:" prompt. This notice can contain up to 1024 characters and new lines.<br>**Command mode**: Global configuration |
| **[no] banner** *<1-80 characters>* | Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed.<br>**Command mode**: Global configuration |
| **[no] hostname** *<string>* | Enables or disables displaying of the host name (system administrator's name) in the command line interface.<br>**Command mode**:: Global configuration |
| **[no] system bootp** | Enables or disables the use of BOOTP. If you enable BOOTP, the switch will query its BOOTP server for all of the switch IP parameters. The default value is `enabled`.<br>**Command mode**: Global configuration |
| **[no] system dhcp** | Enables or disables Dynamic Host Control Protocol for setting the management IP address on interface 256. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default value is `enabled`.<br>**Command mode**: Global configuration |
| **[no] enable** *<string>* | Allows administrators to assign the Privilege EXEC password. The password will be required to enter Privilege EXEC mode. The default value is `disabled`.<br>**Command mode**: Global configuration |
| **show system** | Displays the current system parameters.<br>**Command mode**: All except User EXEC |

# System host log configuration

The following table describes the Syslog Configuration commands.

Table 78 Syslog Configuration commands

| Command | Description |
|---|---|
| **[no] logging host** <*1-2*> **address** <*IP address*> | Sets the IP address of the first or second syslog host. For example, 100.10.1.1<br>**Command mode**: Global configuration |
| **logging host** <*1-2*> **severity** <*1-7*> | Sets the severity level of the first or second syslog host displayed. The default is 7, which means log all the severity levels.<br>**Command mode**: Global configuration |
| **logging host** <*1-2*> **facility** <*1-7*> | This option sets the facility level of the first or seconds syslog host displayed. The default is 0.<br>**Command mode**: Global configuration |
| **[no] logging console** | Enables or disables delivering syslog messages to the console. When necessary, disabling console ensures the switch is not affected by syslog messages. It is enabled by default.<br>**Command mode**: Global configuration |
| **[no] logging log {**<*feature*>**}** | Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features or enable/disable syslog on all available features. Features include:<br>• cfg<br>• cli<br>• console<br>• dot1x<br>• ip<br>• management<br>• ntp<br>• ospf<br>• rmon<br>• spanning-tree-group<br>• ssh<br>• system<br>• ufd<br>• vlan<br>• vrrp<br>• web<br>**Command mode**: Global configuration |
| **show logging** | Displays the current syslog settings.<br>**Command mode**: All |

# Secure Shell Server configuration

Telnet traffic on the network is not secure. These commands enable Secure Shell (SSH) access from any SSH client. The SSH program securely logs into another computer over a network and executes commands in a secure environment. All data using SSH is encrypted.

Secure Shell can be configured on the switch using the console port and Telnet only. The commands are not available if you access the switch using the Browser-based Interface (BBI).

NOTE: See the *N8406-023 1Gb Intelligent L3 Switch Application Guide* for information on SSH.

The following table describes the SSHD Configuration commands.

Table 79 SSHD Configuration commands

| Command | Description |
|---|---|
| **ssh interval** *<0-24>* | Defines interval for auto-generating the RSA server key. The switch will auto-generate the RSA server key at the interval defined in this command. The range is 0-24 hours.<br>The value of zero (0) means the RSA server key auto-generation is disabled. If the switch has been busy performing any other key generation and the assigned time of interval expires, the RSA server will skip generating the key.<br>**Command mode**: Global configuration |
| **ssh scp-password** | Defines the administrator password that is for Secure Copy (SCP) only. The username for this SCP administrator is *scpadmin*.<br>Typically, SCP is used to copy files securely from one machine to another. In the switch, SCP is used to download and upload the switch configuration using secure channels.<br>**Command mode**: Global configuration |
| **ssh generate-host-key** | Generates the RSA host keys manually. The switch creates this key automatically while configuring the switch with Secure Shell (SSH). But you can generate the key manually by using this command if you need to overwrite the key for security reasons. The command will take effect immediately.<br>**Command mode**: Global configuration |
| **ssh generate-server-key** | Generates the RSA server key. The switch creates this key automatically while configuring the switch with Secure Shell (SSH). You can generate the key manually by using this command if you need to overwrite the key for security reasons. The command will take effect immediately.<br>**Command mode**: Global configuration |
| **ssh port** *<TCP port number>* | Sets the SSH server port number.<br>**Command mode**: Global configuration |
| **ssh scp-enable** | Enables the SCP apply and save.<br>**Command mode**: Global configuration |
| **no ssh scp-enable** | Disables the SCP apply and save. This is the default for SCP.<br>**Command mode**: Global configuration |
| **ssh enable** | Enables the SSH server.<br>**Command mode**: Global configuration |
| **no ssh enable** | Disables the SSH server. This is the default for the SSH server.<br>**Command mode**: Global configuration |
| **show ssh** | Displays the current SSH server configuration.<br>**Command mode**: All except User EXEC |

# RADIUS server configuration

NOTE: See the *N8406-023 1Gb Intelligent L3 Switch Application Guide* for information on RADIUS.

The following table describes the RADIUS Server Configuration commands.

Table 80 RADIUS Server Configuration commands

| Command | Description |
|---|---|
| **[no] radius-server primary-host** *<IP address>* **key** *<1-32 characters>* | Sets the primary RADIUS server address and shared secret between the switch and the RADIUS server(s).<br>**Command mode**: Global configuration |
| **[no] radius-server secondary-host** *<IP address>* **key** *<1-32 characters>* | Sets the secondary RADIUS server address and shared secret between the switch and the RADIUS server(s).<br>**Command mode**: Global configuration |
| **radius-server port** *<UDP port number>* | Enter the number of the User Datagram Protocol (UDP) port to be configured, between 1500-3000. The default is 1645.<br>**Command mode**: Global configuration |
| **radius-server retransmit** *<1-3>* | Sets the number of failed authentication requests before switching to a different RADIUS server. The range is 1-3 requests. The default is 3 requests.<br>**Command mode**: Global configuration |
| **radius-server timeout** *<1-10>* | Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The range is 1-10 seconds. The default is 3 seconds.<br>**Command mode**: Global configuration |
| **[no] radius-server telnet-backdoor** | Enables or disables the RADIUS back door for telnet/SSH/ HTTP/HTTPS. The default is disabled. This command does not apply when secure backdoor is enabled.<br>**Command mode**: Global configuration |
| **[no] radius-server secure-backdoor** | Enables or disables the RADIUS back door using secure password for telnet/SSH/ HTTP/HTTPS. The default is disabled. This command does not apply when backdoor (`telnet`) is enabled.<br>**Command mode**: Global configuration |
| **radius-server enable** | Enables the RADIUS server.<br>**Command mode**: Global configuration |
| **no radius-server enable** | Disables the RADIUS server. This is the default.<br>**Command mode**: Global configuration |
| **show radius-server** | Displays the current RADIUS server parameters.<br>**Command mode**: All except User EXEC |

IMPORTANT: If RADIUS is enabled, you must login using RADIUS authentication when connecting via the console or Telnet/SSH/HTTP/HTTPS. Backdoor for console is always enabled, so you can connect using noradius and the administrator password even if the backdoor (`telnet`) or secure backdoor (`secbd`) are disabled.

If Telnet backdoor is enabled (`telnet ena`), type in `noradius` as a backdoor to bypass RADIUS checking, and use the administrator password to log into the switch. The switch allows this even if RADIUS servers are available.

If secure backdoor is enabled (`secbd ena`), type in `noradius` as a backdoor to bypass RADIUS checking, and use the administrator password to log into the switch. The switch allows this only if RADIUS servers are not available.

# TACACS+ server configuration

TACACS+ (Terminal Access Controller Access Control System) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols are more secure than the TACACS encryption protocol. TACACS+ is described in RFC 1492.

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports decoupled authentication, authorization, and accounting.

The following table describes the TACACS+ Server Configuration commands.

Table 81 TACACS+ Server Configuration commands

| Command | Description |
|---|---|
| **[no] tacacs-server primary-host** *<IP address>* **key** *<1-32 characters>* | Defines the primary TACACS+ server address.<br>**Command mode**: Global configuration |
| **[no] tacacs-server secondary-host** *<IP address>* **key** *<1-32 characters>* | Defines the primary or secondary shared secret between the switch and the TACACS+ server(s).<br>**Command mode**: Global configuration |
| **tacacs-server port** *<TCP port number>* | Enter the number of the TCP port to be configured, between 1 - 65000. The default is 49.<br>**Command mode**: Global configuration |
| **tacacs-server retransmit** *<1-3>* | Sets the number of failed authentication requests before switching to a different TACACS+ server. The range is 1-3 requests. The default is 3 requests.<br>**Command mode**: Global configuration |
| **tacacs-server timeout** *<4-15>* | Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The range is 4-15 seconds. The default is 5 seconds.<br>**Command mode**: Global configuration |
| **[no] tacacs-server telnet-backdoor** | Enables or disables the TACACS+ back door for telnet. The `telnet` command also applies to SSH/SCP connections and the Browser-based Interface (BBI). The default is disabled. This command does not apply when secure backdoor (`secbd`) is enabled.<br>**Command mode**: Global configuration |
| **[no] tacacs-server secure-backdoor** | Enables or disables the TACACS+ back door using secure password for telnet/SSH/ HTTP/HTTPS. The default is disabled. This command does not apply when backdoor (`telnet`) is enabled.<br>**Command mode**: Global configuration |
| **[no] tacacs-server privilege-mapping** | Enables or disables TACACS+ privilege-level mapping. The default value is `disabled`.<br>**Command mode**: Global configuration |
| **[no] tacacs-server user-mapping <***0-15***> {user\|oper\|admin}** | Maps a TACACS+ authorization level to this switch user level. Enter a TACACS+ privilege level (0-15), followed by the corresponding the user level (user, oper, admin).<br>**Command mode**: Global configuration |
| **tacacs-server enable** | Enables the TACACS+ server.<br>**Command mode:** Global configuration |
| **no tacacs-server enable** | Disables the TACACS+ server. This is the default.<br>**Command mode:** Global configuration |
| **show tacacs-server** | Displays current TACACS+ configuration parameters.<br>**Command mode**: All except User EXEC |

IMPORTANT: If TACACS+ is enabled, you must login using TACACS+ authentication when connecting via the console or Telnet/SSH/HTTP/HTTPS. Backdoor for console is always enabled, so you can connect using `notacacs` and the administrator password even if the backdoor (`telnet`) or secure backdoor (`secbd`) are disabled.

If Telnet backdoor is enabled (`telnet ena`), type in `notacacs` as a backdoor to bypass TACACS+ checking, and use the administrator password to log into the switch. The switch allows this even if TACACS+ servers are available.

If secure backdoor is enabled (`secbd ena`), type in `notacacs` as a backdoor to bypass TACACS+ checking, and use the administrator password to log into the switch. The switch allows this only if TACACS+ servers are not available.

## NTP server configuration

These commands enable you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

The following table describes the NTP Server Configuration commands.

Table 82 NTP Server Configuration commands

| Command | Description |
|---|---|
| **[no] ntp primary-server** *<IP address>* | Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock. For example, 100.10.1.1<br>**Command mode**: Global configuration |
| **[no] ntp secondary-server** *<IP address>* | Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock. For example, 100.10.1.2<br>**Command mode**: Global configuration |
| **ntp interval** *<1-44640>* | Specifies the interval, in minutes (1-44640), to resynchronize the switch clock with the NTP server. The default is 1440 seconds.<br>**Command mode**: Global configuration |
| **system timezone** *<hh:mm>* | Configures the NTP time zone offset from Greenwich Mean Time (GMT), in hours and minutes. The offset format is HH:MM.<br>**Command mode**: Global configuration |
| **ntp enable** | Enables the NTP synchronization service.<br>**Command mode**: Global configuration |
| **no ntp enable** | Disables the NTP synchronization service. This is the default.<br>**Command mode**: Global configuration |
| **show ntp** | Displays the current NTP service settings.<br>**Command mode**: All |

# System SNMP configuration

The switch software supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

- SNMP parameters that can be modified include:
- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string

The following table describes the System SNMP Configuration commands. The following sections provide more detailed information and commands.

Table 83 System SNMP Configuration commands

| Command | Description |
|---|---|
| **[no] hostname** *<1-64 characters>* | Configures the name for the system. The name can have a maximum of 64 characters.<br>**Command mode**: Global configuration |
| **[no] snmp-server location** *<1-64 characters>* | Configures the name of the system location. The location can have a maximum of 64 characters.<br>**Command mode**: Global configuration |
| **[no] snmp-server contact** *<1-64 characters>* | Configures the name of the system contact. The contact can have a maximum of 64 characters.<br>**Command mode**: Global configuration |
| **snmp-server read-community** *<1-32 characters>* | Configures the SNMP read community string. The read community string controls SNMP “get” access to the switch. It can have a maximum of 32 characters. The default read community string is *public*.<br>**Command mode**: Global configuration |
| **snmp-server write-community** *<1-32 characters>* | Configures the SNMP write community string. The write community string controls SNMP “set” and “get” access to the switch. It can have a maximum of 32 characters. The default write community string is *private*.<br>**Command mode**: Global configuration |
| **snmp-server timeout** *<1-30>* | Sets the timeout value for the SNMP state machine. The range is 1-30 minutes. The default value is 5 minutes.<br>**Command mode**: Global configuration |
| **[no] snmp-server authentication-trap enable** | Enables or disables the use of the system authentication trap facility. The default setting is disabled.<br>**Command mode**: Global configuration |
| **[no] snmp-server link-trap <***1-24***> enable** | Enables or disables the sending of SNMP link up and link down traps. The default setting is enabled.<br>**Command mode**: Global configuration |
| **[no] snmp-server ufd-trap** | Enables or disables the sending of Uplink Failure Detection traps. The default setting is disabled.<br>**Command mode**: Global configuration |
| **show snmp-server** | Displays the current SNMP configuration.<br>**Command mode**: All |

# SNMPv3 configuration

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please see RFC2271 to RFC2275.

The following table describes the SNMPv3 Configuration commands.

Table 84 SNMPv3 Configuration commands

| Command | Description |
|---|---|
| **snmp-server user** *<1-16>* | Configures a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. The range is 1-16.<br>**Command mode**: Global configuration |
| **snmp-server view** *<1-128>* | Configures different MIB views. The range is 1-128.<br>**Command mode**: Global configuration |
| **snmp-server access** *<1-32>* | Configures access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. The range is 1-32.<br>**Command mode**: Global configuration |
| **snmp-server group** *<1-16>* | Configures an SNMP group. A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. The range is 1-16.<br>**Command mode**: Global configuration |
| **snmp-server community** *<1-16>* | Configures a community table entry. The community table contains objects for mapping community strings and version-independent SNMP message parameters. The range is 1-16.<br>**Command mode**: Global configuration |
| **snmp-server target-address** *<1-16>* | Configures the destination address and user security levels for outgoing notifications. This is also called the transport endpoint. The range is 1-16.<br>**Command mode**: Global configuration |
| **snmp-server target-parameters** *<1-16>* | Configures SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. The range is 1-16.<br>**Command mode**: Global configuration |
| **snmp-server notify** *<1-16>* | Configures a notification index. A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. The range is 1-16.<br>**Command mode**: Global configuration |
| **snmp-server version {v1v2v3\|v3only}** | Enables or disables the access to SNMP version 1 and version 2. This command is enabled by default (v1v2v3).<br>**Command mode**: Global configuration |
| **show snmp-server v3** | Displays the current SNMPv3 configuration.<br>**Command mode**: All |

## SNMPv3 User Security Model configuration

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

These commands help you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

The following table describes the User Security Model Configuration commands.

Table 85 User Security Model Configuration commands

| Command | Description |
|---|---|
| **snmp-server user** *<1-16>* **name** *<1-32 characters>* | Configures a string up to 32 characters long that represents the name of the user. This is the login name that you need in order to access the switch.<br>**Command mode**: Global configuration |
| **snmp-server user** *<1-16>* **authentication-protocol {md5\|sha\|none} [authentication-password** *<password>***]** | Configures the authentication protocol and password.<br>The authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96, or none. The default algorithm except usmUser 1-2 is `none`.<br>When you configure an authentication algorithm, you must provide a password, otherwise you receive an error message during validation. This command allows you to create or change your password for authentication.<br>**Command mode**: Global configuration |
| **snmp-server user** *<1-16>* **privacy-protocol {des\|none} [privacy-password** *<password>***]** | Configures the type of privacy protocol and the privacy password.<br>The privacy protocol protects messages from disclosure. The options are `des` (CBC-DES Symmetric Encryption Protocol) or `none`. If you specify `des` as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select `none` as the authentication protocol, you receive an error message.<br>You can create or change the privacy password.<br>**Command mode**: Global configuration |
| **no snmp-server user** *<1-16>* | Deletes the USM user entries.<br>**Command mode**: Global configuration |
| **show snmp-server v3 user** | Displays the USM user entries.<br>**Command mode**: All |

## SNMPv3 View configuration

The following table describes the SNMPv3 View Configuration commands.

Table 86 SNMPv3 View Configuration commands

| Command | Description |
|---|---|
| **snmp-server view** *<1-128>* **name** *<1-32 characters>* | Defines the name for a family of view subtrees up to a maximum of 32 characters.<br>**Command mode**: Global configuration |
| **snmp-server view** *<1-128>* **tree** *<1-64 characters>* | Defines the Object Identifier (OID), a string of maximum 64 characters, which when combined with the corresponding mask defines a family of view subtrees.<br>An example of an OID is `1.3.6.1.2.1.1.1.0`<br>**Command mode**: Global configuration |
| **snmp-server view** *<1-128>* **mask** *<1-32 characters>* | Defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees. The mask can have a maximum of 32 characters.<br>**Command mode**: Global configuration |
| **snmp-server view** *<1-128>* **type {included\|excluded}** | Selects whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` define a family of view subtrees, which is included in or excluded from the MIB view.<br>**Command mode**: Global configuration |
| **no snmp-server view** *<1-128>* | Deletes the `vacmViewTreeFamily` group entry.<br>**Command mode**: Global configuration |
| **show snmp-server v3 view** | Displays the current `vacmViewTreeFamily` configuration.<br>**Command mode**: All |

# SNMPv3 View-based Access Control Model configuration

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

The following table describes the User Access Control Configuration commands.

Table 87 View-based Access Control Configuration commands

| Command | Description |
|---|---|
| **snmp-server access** *<1-32>* **name** *<1-32 characters>* | Defines the name of the group, up to a maximum of 32 characters.<br>**Command mode**: Global configuration |
| **snmp-server access** *<1-32>* **security {usm\|snmpv1\|snmpv2}** | Allows you to select the security model to be used.<br>**Command mode**: Global configuration |
| **snmp-server access** *<1-32>* **level {noAuthNoPriv\|authNo-Priv\|authPriv}** | Defines the minimum level of security required to gain access rights. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol.<br>**Command mode**: Global configuration |
| **snmp-server access** *<1-32>* **read-view** *<1-32 characters>* | Defines a 32 character long read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.<br>**Command mode**: Global configuration |
| **snmp-server access** *<1-32>* **write-view** *<1-32 characters>* | Defines a 32 character long write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.<br>**Command mode**: Global configuration |
| **snmp-server access** *<1-32>* **notify-view** *<1-32 characters>* | Defines a 32 character long notify view name that allows you notify access to the MIB view.<br>Command mode: Global configuration |
| **no snmp-server access** *<1-32>* | Deletes the View-based Access Control entry.<br>**Command mode**: Global configuration |
| **show snmp-server v3 access** | Displays the View-based Access Control configuration.<br>**Command mode**: All |

# SNMPv3 Group configuration

The following table describes the SNMPv3 Group Configuration commands.

Table 88 SNMPv3 Group Configuration commands

| Command | Description |
|---|---|
| **snmp-server group** *<1-16>* **security {usm\|snmpv1\|snmpv2}** | Defines the security model.<br>**Command mode**: Global configuration |
| **snmp-server group** *<1-16>* **user-name** *<1-32 characters>* | Sets the user name. The user name can have a maximum of 32 characters.<br>**Command mode**: Global configuration |
| **snmp-server group** *<1-16>* **group-name** *<1-32 characters>* | The name for the access group. The group name can have a maximum of 32 characters.<br>**Command mode**: Global configuration |
| **no snmp-server group** *<1-16>* | Deletes the `vacmSecurityToGroup` entry.<br>**Command mode**: Global configuration |
| **show snmp-server v3 group** | Displays the current `vacmSecurityToGroup` configuration.<br>**Command mode**: All |

# SNMPv3 Community Table configuration

These commands are used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

The following table describes the SNMPv3 Community Table Configuration commands.

Table 89 SNMPv3 Community Table Configuration commands

| Command | Description |
|---|---|
| **snmp-server community** *<1-16>* **index** *<1-32 characters>* | Configures the unique index value of a row in this table. The index can have a maximum of 32 characters.<br>**Command mode**: Global configuration |
| **snmp-server community** *<1-16>* **name** *<1-32 characters>* | Defines a readable 32 character string that represents the corresponding value of an SNMP community name in a security model.<br>**Command mode**: Global configuration |
| **snmp-server community** *<1-16>* **user-name** *<1-32 characters>* | Sets the user name, up to 32 characters.<br>**Command mode**: Global configuration |
| **snmp-server community** *<1-16>* **tag** *<1-255 characters>* | Configures a tag of up to 255 characters maximum. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap.<br>**Command mode**: Global configuration |
| **no snmp-server community** *<1-16>* | Deletes the community table entry.<br>**Command mode**: Global configuration |
| **show snmp-server v3 community** | Displays the community table configuration.<br>**Command mode**: All |

# SNMPv3 Target Address Table configuration

The following table describes the SNMPv3 Target Address Table Configuration commands.

Table 90 SNMPv3 Target Address Table Configuration commands

| Command | Description |
|---|---|
| **snmp-server target-address** *<1-16>* **address** *<transport IP address>* **name** *<1-32 characters>* | Configures the locally arbitrary, but unique identifier, target address name associated with this entry.<br>**Command mode**: Global configuration |
| **snmp-server target-address** *<1-16>* **name** *<1-32 characters>* **address** *<transport IP address>* | Configures a transport address IP that can be used in the generation of SNMP traps.<br>**Command mode**: Global configuration |
| **snmp-server target-address** *<1-16>* **port** *<transport address port>* | Configures a transport address port that can be used in the generation of SNMP traps.<br>**Command mode**: Global configuration |
| **snmp-server target-address** *<1-16>* **taglist** *<1-255 characters>* | Configures a list of tags (up to 255 characters maximum) that are used to select target addresses for a particular operation.<br>**Command mode**: Global configuration |
| **snmp-server target-address** *<1-16>* **parameters-name** *<1-32 characters>* | Sets the parameter name.<br>**Command mode**: Global configuration |
| **no snmp-server target-address** *<1-16>* | Deletes the Target Address Table entry.<br>**Command mode**: Global configuration |
| **show snmp-server v3 target-address** | Displays the current Target Address Table configuration.<br>**Command mode**: All |

## SNMPv3 Target Parameters Table configuration

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (noAuthnoPriv, authNoPriv, or authPriv).

The following table describes the SNMPv3 Target Parameters Table Configuration commands.

Table 91 SNMPv3 Target Parameters Table Configuration commands

| Command | Description |
|---|---|
| **snmp-server target-parameters** *<1-16>* **name** *<1-32 characters>* | Configures the locally arbitrary, but unique identifier that is associated with this entry.<br>**Command mode**: Global configuration |
| **snmp-server target-parameters** *<1-16>* **message {snmpv1\|snmpv2c\|snmpv3}** | Configures the message processing model that is used to generate SNMP messages.<br>**Command mode**: Global configuration |
| **snmp-server target-parameters** *<1-16>* **security {usm\|snmpv1\|snmpv2}** | Selects the security model to be used when generating the SNMP messages.<br>**Command mode**: Global configuration |
| **snmp-server target-parameters** *<1-16>* **user-name** *<1-32 characters>* | Defines the name that identifies the user in the USM table, on whose behalf the SNMP messages are generated using this entry.<br>**Command mode**: Global configuration |
| **snmp-server target-parameters** *<1-16>* **level {noAuthNo-Priv\|authNoPriv\|authPriv}** | Selects the level of security to be used when generating the SNMP messages using this entry. The level noAuthNoPriv means that the SNMP message will be sent without authentication and without using a privacy protocol. The level authNoPriv means that the SNMP message will be sent with authentication but without using a privacy protocol. The authPriv means that the SNMP message will be sent both with authentication and using a privacy protocol.<br>**Command mode**: Global configuration |
| **no snmp-server target-parameters** *<1-16>* | Deletes the targetParamsTable entry.<br>**Command mode**: Global configuration |
| **show snmp-server v3 target-parameters** | Displays the current targetParamsTable configuration.<br>**Command mode**: All |

## SNMPv3 Notify Table configuration

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

The following table describes the SNMPv3 Notify Table Configuration commands.

Table 92 SNMPv3 Notify Table Configuration commands

| Command | Description |
|---|---|
| **snmp-server notify** *<1-16>* **name** *<1-32 characters>* | Defines a locally arbitrary but unique identifier associated with this SNMP notify entry.<br>**Command mode**: Global configuration |
| **snmp-server notify** *<1-16>* **tag** *<1-255 characters>* | Defines a tag of 255 characters maximum that contains a tag value which is used to select entries in the Target Address Table. Any entry in the snmpTargetAddrTable, that matches the value of this tag, is selected.<br>**Command mode**: Global configuration |
| **no snmp-server notify** *<1-16>* | Deletes the notify table entry.<br>**Command mode**: Global configuration |
| **show snmp-server v3 notify** | Displays the current notify table configuration.<br>**Command mode**: All |

## System Access configuration

The following table describes the System Access Configuration commands.

Table 93 System Access Configuration commands

| Command | Description |
|---|---|
| **[no] access http enable** | Enables or disables HTTP (Web) access to the Browser-based Interface. It is enabled by default.<br>**Command mode**: Global configuration |
| **access http port** *<TCP port number>* | Sets the switch port used for serving switch Web content. The default is HTTP port 80.<br>**Command mode**: Global configuration |
| **[no] access snmp {read-only\|read-write}** | Disables or provides read-only/write-read SNMP access.<br>**Command mode**: Global configuration |
| **[no] access telnet enable** | Enables or disables telnet server. It is enabled by default.<br>**Command mode**: Global configuration |
| **access telnet port** *<TCP port number>* | Sets an optional telnet server port number for cases where the server listens for telnet sessions on a non-standard port. The default is 23.<br>**Command mode**: Global configuration |
| **access tftp-port** *<TFTP port number>* | Sets an optional telnet server port number for cases where the server listens for TFTP sessions on a non-standard port. The default is 69.<br>**Command mode**: Global configuration |
| **show access** | Displays the current system access parameters.<br>**Command mode**: All except User EXEC |

## Management Networks configuration

The following table describes the Management Networks Configuration commands. You can configure up to 10 management networks on the switch.

Table 94 Management Networks Configuration commands

| Command | Description |
|---|---|
| **access management-network** *<IP address> <IP mask>* | Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation.<br>**Command mode**: Global configuration |
| **no access management-network** *<IP address> <IP mask>* | Removes a defined network, which consists of a management network address and a management network mask address.<br>**Command mode**: Global configuration |
| **show access management-network** | Displays the current management networks parameters.<br>**Command mode**: All except User EXEC |

## User Access Control configuration

The following table describes the User Access Control commands.

Table 95 User Access Control Configuration commands

| Command | Description |
|---|---|
| **access user eject** *<user name>* | Ejects the selected user from the switch.<br>**Command mode**: Global configuration |
| **access user user-password** | Sets the user (`user`) password (maximum of 128 characters). The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes.<br>**Command mode**: Global configuration |
| **access user operator-password** | Sets the operator (`oper`) password (maximum of 128 characters). The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports or the entire switch.<br>**Command mode**: Global configuration |
| **access user administrator-password** | Sets the administrator (`admin`) password (maximum of 128 characters). The super user administrator has complete access to all information and configuration commands on the switch, including the ability to change both the user and administrator passwords.<br>**Command mode**: Global configuration |
| **show access user** | Displays the current user status.<br>**Command mode**: All except User EXEC |

## User ID configuration

The following table describes the User ID Configuration commands.

Table 96 User ID Configuration commands

| Command | Description |
|---|---|
| **access user** *<1-10>* **level {user\|operator\|administrator}** | Sets the Class-of-Service to define the user's authority level.<br>**Command mode**: Global configuration |
| **access user** *<1-10>* **name** *<1-8 characters>* | Defines the user name of maximum eight characters.<br>**Command mode**: Global configuration |
| **access user** *<1-10>* **password** | Sets the user password of up to 128 characters maximum.<br>**Command mode**: Global configuration |
| **access user** *<1-10>* **enable** | Enables the user ID.<br>**Command mode**: Global configuration |
| **no access user** *<1-10>* **enable** | Disables the user ID.<br>**Command mode**: Global configuration |
| **no access user** *<1-10>* | Deletes the user ID.<br>**Command mode**: Global configuration |
| **show access user** | Displays the current user ID parameters.<br>**Command mode**: All except User EXEC |

# HTTPS Access configuration

The following table describes the HTTPS Access Configuration commands.

Table 97 HTTPS Access Configuration commands

| Command | Description |
|---|---|
| **[no] access https enable** | Enables or disables BBI access (Web access) using HTTPS. The default value is `disabled`.<br>**Command mode**: Global configuration |
| **access https port** *<TCP port number>* | Defines the HTTPS Web server port number. The default is 443.<br>**Command mode**: Global configuration |
| **access https generate-certificate** | Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example:<br>• Country Name (2 letter code) [ ]: JP<br>• State or Province Name (full name) [ ]: Tokyo<br>• Locality Name (for example, city) [ ]: Fuchu<br>• Organization Name (for example, company) [ ]: NEC<br>• Organizational Unit Name (for example, section) [ ]: SIGMABLADE<br>• Common Name (for example, user's name) [ ]: Taro<br>• Email (for example, email address) [ ]: info@nec.com<br>You must confirm if you want to generate the certificate. It takes approximately 30 seconds to generate the certificate. Then the switch restarts SSL agent.<br>**Command mode**: Global configuration |
| **access https save-certificate** | Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.<br>**Command mode**: Global configuration |
| **show access** | Displays the current SSL Web Access configuration.<br>**Command mode**: All except User EXEC |

# Port configuration

Use the port configuration commands to configure settings for individual switch ports.

NOTE: Port 19 is reserved for switch management interface.

The following table describes the Port Configuration commands. The following sections provide more detailed information and commands.

Table 98 Port Configuration commands

| Command | Description |
|---|---|
| **interface gigabitethernet** *<port number>* | Enter Interface Port configuration mode for the selected port.<br>**Command mode**: Global configuration |
| **dot1p <***0-7***>** | Configures the port's 802.1p priority level.<br>**Command mode**: Interface port |
| **pvid** *<1-4095>* | Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number for all ports except Port 19 is 1. Note: VLAN 4095 is reserved for switch management interface.<br>**Command mode**: Interface port |
| **name** *<1-64 characters>* | Sets a name for the port (maximum 64 characters). The assigned port name displays next to the port number on some information and statistics screens.<br>**Command mode**: Interface port |
| **[no] rmon** | Enables or disables Remote Monitoring for the port. The default is disabled. RMON must be enabled for any RMON configurations to function.<br>**Command mode**: Interface port |
| **[no] tagging** | Disables or enables VLAN tagging for this port. It is disabled by default.<br>**Command mode**: Interface port |
| **[no] tag-pvid** | Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default value is enabled.<br>**Command mode**: Interface port |
| **copper** | Configures the port's transmission media as `copper`. This command is available only for Ports 21-24.<br>**Command mode**: Interface port |
| **fiber** | Configures the port's transmission media as `fiber`. This command is available only for Ports 21-24.<br>**Command mode**: Interface port |
| **auto-mode** | Configures the port's transmission media as `auto`. This command is available only for Ports 21-24.<br>**Command mode**: Interface port |
| **[no] broadcast-threshold** *<0-262143>* | Limits the number of broadcast packets per second to the specified value. If disabled (`no`), the port forwards all broadcast packets.<br>**Command mode**: Interface port |
| **[no] multicast-threshold** *<0-262143>* | Limits the number of multicast packets per second to the specified value. If disabled (`no`), the port forwards all multicast packets.<br>**Command mode**: Interface port |
| **[no] dest-lookup-threshold** *<0-262143>* | Limits the number of unknown unicast packets per second to the specified value. If disabled (`no`), the port forwards all unknown unicast packets.<br>**Command mode**: Interface port |
| **no shutdown** | Enables the port.<br>**Command mode**: Interface port |
| **shutdown** | Disables the port. To temporarily disable a port without changing its configuration attributes, see the "Temporarily disabling a port" section later in this chapter.<br>**Command mode**: Interface port |
| **show interface gigabitethernet** *<port number>* | Displays current port parameters.<br>**Command mode**: All |

## Temporarily disabling a port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
Switch# interface gigabitethernet <port number> shutdown
```

Because this configuration sets a temporary state for the port, you do not need to perform a save operation. The port state reverts to its original configuration when the switch is reloaded.

## Port link configuration

Use these commands to set port parameters for the port link.

Link commands are described in the following table. Using these commands, you can set port parameters such as speed, duplex, flow control, and negotiation mode for the port link.

The following table describes the Gigabit Link Configuration commands.

Table 99 Gigabit Link Configuration commands

| Command | Description |
|---|---|
| **speed {10\|100\|1000\|auto}** | Sets the link speed. Not all options are valid on all ports. The choices include:<br>• 10 Mb/s<br>• 100 Mb/s<br>• 1000 Mb/s<br>• "auto," for automatic detection (default)<br>Note: Ports 1-18 are set to 1000 Mb/s, and cannot be changed.<br>**Command mode**: Interface port |
| **duplex {full\|half\|any}** | Sets the operating mode. Not all options are valid on all ports. The choices include:<br>• Full-duplex<br>• Half-duplex<br>• "Any," for automatic detection (default)<br>Note: Ports 1-16 are set to "Any" and Ports 17-18 are set to full duplex. These ports cannot be changed.<br>**Command mode**: Interface port |
| **flowcontrol {receive\|send\|both}** | Sets the flow control. The choices include:<br>• Receive (rx) flow control<br>• Transmit (tx) flow control<br>• Both receive and transmit flow control (default)<br>**Command mode**: Interface port |
| **no flowcontrol** | Sets the flow control to none.<br>**Command mode**: Interface port |
| **[no] auto** | Enables or disables auto-negotiation for the port. The default is enabled.<br>**Command mode**: Interface port |
| **show interface gigabitethernet** *<port number>* | Displays current port parameters.<br>**Command mode**: All |

## ACL Port configuration

The following table describes the basic Access Control List Configuration commands for the port.

Table 100 ACL Port Configuration commands

| Command | Description |
|---|---|
| **[no] access-control list <***1-762***>** | Adds or removes the specified ACL.<br>**Command mode:** Interface port |
| **[no] access-control group <***1-762***>** | Adds or removes the specified ACL Group.<br>**Command mode:** Interface port |
| **show interface gigabitethernet [<***port number***>] access-control** | Displays current ACL QoS parameters.<br>**Command mode:** All |

# Layer 2 configuration

The following table describes the Layer 2 Configuration commands. The following sections provide more detailed information and commands.

Table 101 Layer 2 Configuration commands

| Command | Description |
|---|---|
| **vlan** *<1-4095>* | Enter VLAN configuration mode.<br>**Command mode**: Global configuration |
| **[no] spanning-tree uplinkfast** | Enables or disables Fast Uplink Convergence, which provides rapid Spanning Tree convergence to an upstream switch during failover. The default is disabled.<br>**Note**: When enabled, this feature increases bridge priorities to 65500 for all STGs except STG 128 and path cost by 3000 for all external STP ports.<br>**Command mode**: Global configuration |
| **spanning-tree uplinkfast max-update-rate** *<10-200>* | Configures the station update rate, in packets per second. The range is 10-200. The default value is 40.<br>**Command mode**: Global configuration |
| **show layer2** | Displays current Layer 2 parameters.<br>**Command mode**: All |

# 802.1x configuration

This feature allows you to configure this switch as an IEEE 802.1x Authenticator, to provide port-based network access control. The following table describes the 802.1x Configuration commands.

Table 102 802.1x Configuration commands

| Command | Description |
|---|---|
| **dot1x enable** | Globally enables 802.1x.<br>**Command mode**: Global configuration |
| **no dot1x enable** | Globally disables 802.1x. This is the default.<br>**Command mode**: Global configuration |
| **show dot1x** | Displays current 802.1x parameters.<br>**Command mode**: All |

# 802.1x Global configuration

The global 802.1x commands allow you to configure parameters that affect all ports in the switch. The following table describes the 802.1x Global Configuration commands.

Table 103 802.1x Global Configuration commands

| Command | Description |
|---|---|
| **dot1x mode {[force-unauthorized\|auto\|force-authorized]}** | Sets the type of access control for all ports:<br>• **force-unauth** - the port is unauthorized unconditionally.<br>• **auto** - the port is unauthorized until it is successfully authorized by the RADIUS server.<br>• **force-auth** - the port is authorized unconditionally, allowing all traffic.<br>The default value is `force-auth`.<br>**Command mode:** Global configuration |
| **dot1x quiet-time <***0-65535***>** | Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.<br>**Command mode:** Global configuration |
| **dot1x transmit-interval <***1-65535***>** | Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.<br>**Command mode:** Global configuration |
| **dot1x supplicant-timeout <***1-65535***>** | Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet to the authentication server. The default value is 30 seconds. |
| **dot1x server-timeout <***1-65535***>** | Sets the time, in seconds, the authenticator waits for a response from the Radius server before declaring an authentication timeout. The default value is 30 seconds.<br>The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of radius-server timeout (default is 3 seconds).<br>**Command mode**: Global configuration |
| **dot1x max-request <***1-10***>** | Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.<br>**Command mode**: Global configuration |
| **dot1x re-authentication-interval <***1-604800***>** | Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.<br>**Command mode:** Global configuration |
| **[no] dot1x re-authenticate** | Sets the re-authentication status to `on` or `off`. The default value is `off`.<br>**Command mode**: Global configuration |
| **default dot1x** | Resets the global 802.1x parameters to their default values.<br>**Command mode:** Global configuration |
| **show dot1x** | Displays current global 802.1x parameters.<br>**Command mode:** All |

# 802.1x Port configuration

The 802.1x port commands allow you to configure parameters that affect the selected port in the switch. These settings override the global 802.1x parameters.

The following table describes the 802.1x Port Configuration commands.

Table 104 802.1x Port Configuration commands

| Command | Description |
|---|---|
| **dot1x mode {[force-unauthorized\| auto\|force-authorized]}** | Sets the type of access control for the port:<br>• **force-unauth** - the port is unauthorized unconditionally.<br>• **auto** - the port is unauthorized until it is successfully authorized by the RADIUS server.<br>• **force-auth** - the port is authorized unconditionally, allowing all traffic.<br>The default value is `force-auth`.<br>**Command mode**: Interface port |
| **dot1x quiet-time <***0-65535***>** | Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.<br>**Command mode**: Interface port |
| **dot1x transmit-interval <***1-65535***>** | Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.<br>**Command mode:** Interface port |
| **dot1x supplicant-timeout <***1-65535***>** | Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet to the authentication server. The default value is 30 seconds.<br>**Command mode**: Interface port |
| **dot1x server-timeout <***1-65535***>** | Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds.<br>**Command mode**: Interface port |
| **dot1x max-request <***1-10***>** | Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.<br>**Command mode**: Interface port |
| **dot1x re-authentication-interval <***1-604800***>** | Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.<br>**Command mode:** Interface port |
| **[no] dot1x re-authenticate** | Sets the re-authentication status to `on` or `off`. The default value is `off`.<br>**Command mode**: Interface port |
| **default dot1x** | Resets the global 802.1x parameters to their default values.<br>**Command mode**: Interface port |
| **show dot1x** | Displays current global 802.1x parameters.<br>**Command mode**: All |

# Rapid Spanning Tree Protocol / Multiple Spanning Tree Protocol configuration

The switch supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). MSTP allows you to map many VLANs to a small number of spanning tree groups, each with its own topology.

You can configure up to 32 spanning tree groups on the switch.

NOTE: When Multiple Spanning Tree is turned on, VLAN 1 is moved from Spanning Tree Group 1 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 1 is moved back to Spanning Tree Group 1.

The following table describes the Multiple Spanning Tree Configuration commands.

Table 105 Multiple Spanning Tree Configuration commands

| Command | Description |
|---|---|
| **[no] spanning-tree mstp name** *<1-32 characters>* | Configures a name for the MSTP region. All devices within a MSTP region must have the same region name.<br>**Command mode**: Global configuration |
| **spanning-tree mstp version** *<0-65535>* | Configures the revision level for the MSTP region. The revision level is used as a numerical identifier for the region. All devices within a MSTP region must have the same revision level number. The range is 0-65535. The default value is 1.<br>**Command mode**: Global configuration |
| **spanning-tree mstp maximum-hop** *<4-60>* | Configures the maximum number of bridge hops a packet may to traverse before it is dropped. The range is from 4 to 60 hops. The default is 20.<br>**Command mode**: Global configuration |
| **spanning-tree mode {mst\|rstp\|pvst}** | Selects either Rapid Spanning Tree mode, as follows:<br>• Rapid Spanning Tree mode (rstp)<br>• Multiple Spanning Tree mode (mstp).<br>• Per VLAN Spanning Tree (pvst)<br>The default mode is pvst.<br>**Command mode**: Global configuration |
| **show spanning-tree mstp mrst** | Displays the current RSTP/MSTP configuration.<br>**Command mode**: All |

NOTE:

- IEEE 802.1w standard-based RSTP implementation runs on one STG (i.e. same as one spanning tree instance) only. As a result, if 'rstp' mode is selected, then only a single RSTP instance (default for STG 1) is supported for all VLANs, including the Default VLAN 1.
- If multiple spanning tree instances are required, then select 'mstp' mode so that multiple VLANs are handled by multiple spanning tree instances, as specified by IEEE 802.1s standard-based MSTP implementation.
- IEEE 802.1s MSTP supports rapid convergence using IEEE 802.1w RSTP.
- PVST+ does not support rapid convergence in current versions.

NOTE:

The following configurations are unsupported:

- PVST+ (default Spanning Tree setting) is NOT interoperable with Cisco Rapid PVST+.
- MSTP/RSTP (with mode set to either 'mstp' or 'rstp') is NOT interoperable with Cisco Rapid PVST+.

The following configurations are supported:

- PVST+ (default Spanning Tree setting) is interoperable with Cisco PVST+.
- MSTP/RSTP (with mode set to 'mstp') is interoperable with Cisco MST/RSTP.

## Common Internal Spanning Tree configuration

The Common Internal Spanning Tree (CIST) provides compatibility with different MSTP regions and with devices running different Spanning Tree instances. It is equivalent to Spanning Tree Group 0.

The following table describes the commands used to configure CIST commands.

Table 106 CIST Configuration commands

| Command | Description |
|---|---|
| **spanning-tree mstp cist-add-vlan** *<1-4095>* | Adds VLANs to the CIST. Enter one VLAN per line, and press Enter to add the VLANs.<br>**Command mode**: Global configuration |
| **default spanning-tree mstp cist** | Resets all CIST parameters to their default values.<br>**Command mode**: Global configuration |
| **show spanning-tree mstp cist** | Displays the current CIST configuration.<br>**Command mode**: All |

## CIST bridge configuration

CIST bridge parameters are used only when the switch is in MSTP mode. CIST parameters do not affect operation of STP/PVST+.

The following table describes the commands used to configure CIST Bridge Configuration commands.

Table 107 CIST Bridge Configuration commands

| Command | Description |
|---|---|
| **spanning-tree mstp cist-bridge priority** *<0-65535>* | Configures the CIST bridge priority. The bridge priority parameter controls which bridge on the network is the MSTP root bridge.<br>To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768.<br>This command does not apply to RSTP. See the "Bridge Spanning Tree configuration" section for more information.<br>**Command mode**: Global configuration |
| **spanning-tree mstp cist-bridge maximum-age** *<6-40>* | Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds.<br>This command does not apply to RSTP. See the "Bridge Spanning Tree configuration" section for more information.<br>**Command mode**: Global configuration |
| **spanning-tree mstp cist-bridge forward-delay** *<4-30>* | Configures the CIST bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.<br>This command does not apply to RSTP. See the "Bridge Spanning Tree configuration" section for more information.<br>**Command mode**: Global configuration |
| **show spanning-tree mstp cist** | Displays the current CIST bridge configuration.<br>**Command mode**: All |

# CIST port configuration

CIST port parameters are used to modify MRST operation on an individual port basis. CIST parameters do not affect operation of STP/PVST+.

For each port, CIST is turned on by default. Port parameters include:

- Port priority
- Port path cost
- Port Hello time
- Link type
- Edge
- On and off
- Current port configuration

The port option of MRST is turned on by default.

The following table describes the commands used to configure CIST Port Configuration commands.

Table 108 CIST Port Configuration commands

| Command | Description |
|---|---|
| **spanning-tree mstp cist interface-priority** *<0-240>* | Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.<br>**Command mode**: Interface port |
| **spanning-tree mstp cist path-cost** *<0-200000000>* | Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. The default is 20000 for Gigabit ports.<br>**Command mode**: Interface port |
| **spanning-tree mstp cist hello** *<1-10>* | Configures the CIST port Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.<br>**Command mode**: Interface port |
| **spanning-tree mstp cist link-type {auto\|p2p\|shared}** | Defines the type of link connected to the port, as follows:<br>• auto: Configures the port to detect the link type, and automatically match its settings.<br>• p2p: Configures the port for Point-To-Point protocol.<br>• shared: Configures the port to connect to a shared medium (usually a hub).<br>The default link type is auto.<br>**Command mode**: Interface port |
| **[no] spanning-tree mst cist edge** | Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). By default, Ports 1-16 are configured as edge ports.<br>**Command mode**: Interface port |
| **spanning-tree mst cist enable** | Enables CIST on the port. Ports 17-18 and 20-24 are enabled by default.<br>**Command mode**: Interface port |
| **no spanning-tree mst cist enable** | Disables CIST on the port.<br>**Command mode**: Interface port |
| **show interface gigabitethernet** *<port number>* **spanning-tree mstp cist** | Displays the current CIST port configuration.<br>**Command mode**: All |

# Spanning Tree configuration

The switch supports the IEEE 802.1D Spanning Tree Protocol (STP) and Cisco proprietary PVST and PVST+ protocols. You can configure up to 127 spanning tree groups on the switch (STG 128 is reserved for switch management). Spanning Tree is turned on by default.

NOTE: When RSTP is turned on, only STP group 1 can be configured.

The following table describes the Spanning Tree Configuration commands.

Table 109 Spanning Tree Configuration commands

| Command | Description |
|---|---|
| **spanning-tree stp** *<1-128>* **vlan** *<1-4094>* | Associates a VLAN with a spanning tree and requires an external VLAN ID as a parameter.<br>**Command mode**: Global configuration |
| **no spanning-tree stp** *<1-128>* **vlan** *<1-4095>* | Breaks the association between a VLAN and a spanning tree and requires an external VLAN ID as a parameter.<br>**Command mode**: Global configuration |
| **no spanning-tree stp** *<1-128>* **vlan all** | Removes all VLANs from a spanning tree.<br>**Command mode**: Global configuration |
| **spanning-tree stp** *<1-128>* **enable** | Globally enables Spanning Tree Protocol.<br>**Command mode**: Global configuration |
| **no spanning-tree stp** *<1-128>* **enable** | Globally disables Spanning Tree Protocol.<br>**Command mode**: Global configuration |
| **default spanning-tree stp** *<1-128>* | Restores a spanning tree instance to its default configuration.<br>**Command mode**: Global configuration |
| **show spanning-tree stp** *<1-128>* | Displays current Spanning Tree Protocol parameters.<br>**Command mode**: All |

# Bridge Spanning Tree configuration

Spanning tree bridge parameters can be configured for each Spanning Tree Group. STP bridge parameters include:

- Bridge priority
- Bridge hello time
- Bridge maximum age
- Forwarding delay
- Current bridge configuration

The following table describes the Bridge Spanning Tree Configuration commands.

Table 110 Bridge Spanning Tree Configuration commands

| Command | Description |
|---|---|
| **spanning-tree stp** *<1-128>* **bridge priority** *<0-65535>* | Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STP root bridge.<br>To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768.<br>RSTP/MSTP: The range is 0 to 61440, in steps of 4096 (0, 4096, 8192...), and the default is 32768.<br>This command does not apply to MSTP. See the "Common Internal Spanning Tree configuration" section for more information.<br>**Command mode**: Global configuration |
| **spanning-tree stp** *<1-128>* **bridge hello-time** *<1-10>* | Configures the bridge hello time. The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. The range is 1 to 10 seconds, and the default is 2 seconds.<br>This command does not apply to MSTP. See the "Common Internal Spanning Tree configuration" section for more information.<br>**Command mode**: Global configuration |
| **spanning-tree stp** *<1-128>* **bridge maximum-age** *<6-40>* | Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. The range is 6 to 40 seconds, and the default is 20 seconds.<br>This command does not apply to MSTP. See the "Common Internal Spanning Tree configuration" section for more information.<br>**Command mode**: Global configuration |
| **spanning-tree stp** *<1-128>* **bridge forward-delay** *<4-30>* | Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.<br>This command does not apply to MSTP. See the "Common Internal Spanning Tree configuration" section for more information.<br>**Command mode**: Global configuration |
| **show spanning-tree stp** *<1-128>* **bridge** | Displays the current bridge STP parameters.<br>**Command mode**: All |

When configuring STP bridge parameters, the following formulas must be used:

- 2*(*fwd*-1) $\geq$ *mxage*
- 2*(*hello*+1) $\leq$ *mxage*

# Spanning Tree port configuration

By default for STP/PVST+, Spanning tree is turned Off for downlink ports (1-16), and turned On for cross-connect ports (17-18), and uplink ports (20-24). By default for RSTP/MSTP, Spanning tree is turned Off for all downlink ports (1-16) configured as Edge ports, and turned On for cross-connect ports (17-18) and all uplink ports (20-24).

Spanning tree port parameters are used to modify STP operation on an individual port basis. STP port parameters include:

- Port priority
- Port path cost

The following table describes the Spanning Tree Port Configuration commands.

Table 111 Spanning Tree Port Configuration commands

| Command | Description |
|---|---|
| **spanning-tree stp** *<1-128>* **priority** *<0-255>* | Configures the port priority. The port priority helps determine which bridge port becomes the designated port.<br>In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.<br>The range is 0 to 255, and the default is 128.<br>RSTP/MSTP: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128.<br>**Command mode**: Interface port |
| **spanning-tree stp** *<1-128>* **path-cost** *<0-200000000>* | Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost.<br>The range is 0 to 65535. The default is 4 for Gigabit ports except Port 19. A value of 0 indicates that the default cost will be computed for an auto-negotiated link speed. The default cost is 19 for 100Mb/s ports and 4 for Gigabit ports.<br>RSTP/MSTP: The range is 0 – 200000000, and the default is 20000 for Gigabit ports except Port 19.<br>**Command mode**: Interface port |
| **spanning-tree stp** *<1-128>* **link {auto\|p2p\|shared}** | Defines the type of link connected to the port, as follows:<br>• auto: Configures the port to detect the link type, and automatically match its settings.<br>• p2p: Configures the port for Point-To-Point protocol.<br>• shared: Configures the port to connect to a shared medium (usually a hub).<br>This command only applies when RSTP is turned on. See the "Common Internal Spanning Tree configuration" section for more information.<br>**Command mode**: Interface port |
| **[no] spanning-tree stp** *<1-128>* **edge** | Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). By default, Ports 1-16 are configured as edge ports.<br>This command only applies when RSTP is turned on. See the "Common Internal Spanning Tree configuration" section for more information.<br>**Command mode**: Interface port |
| **[no] spanning-tree stp** *<1-128>* **fastforward** | Enables or disables Port Fast Forward on the port. The default is disabled.<br>**Command mode**: Interface port |
| **spanning-tree stp** *<1-128>* **enable** | Enables STP on the port. This is the default for Ports 17-18 and 20-24.<br>**Command mode**: Interface port |
| **no spanning-tree stp** *<1-128>* **enable** | Disables STP on the port.<br>**Command mode**: Interface port |

# Forwarding Database configuration

The following table describes the Forwarding Database Configuration commands.

Table 112 FDB Configuration commands

| Command | Description |
|---|---|
| **mac-address-table aging <***0-65535***>** | Configures the aging value for FDB entries. The default value is 300.<br>**Command mode**: Global configuration |
| **show mac-address-table** | Displays current FDB parameters.<br>**Command mode**: All |

## Static FDB configuration

The following table describes the Static FDB Configuration commands.

Table 113 Static FDB Configuration commands

| Command | Description |
|---|---|
| **mac-address-table static** *<MAC address> <VLAN> <port>* | Adds a static entry to the forwarding database.<br>**Command mode**: Global configuration |
| **no mac-address-table static [***<MAC address>***\|***<VLAN>***]** | Deletes a static entry from the forwarding database.<br>**Command mode**: Global configuration |
| **no mac-address-table static all [mac** *<MAC address>***\|vlan** *<VLAN>***\|port** *<port>***]** | Clears specified static FDB entries from the forwarding database, as follows:<br>• MAC address<br>• VLAN<br>• Port<br>• All<br>**Command mode**: Global configuration |

# Trunk configuration

Trunk groups can provide super-bandwidth connections between switches or other trunk capable devices. A trunk is a group of ports that act together, combining their bandwidth to create a single, larger port. Up to 12 trunk groups can be configured on the switch, with the following restrictions.

- Any physical switch port can belong to no more than one trunk group.
- Up to six ports/trunks can belong to the same trunk group.
- All ports in a trunk must have the same configuration for speed, flow control, and auto negotiation.
- Trunking from other devices must comply with Cisco® EtherChannel® technology.
- By default, port 17 and port 18 are trunked to support an internal switch-to-switch crosslink trunk. By default, ports 17 and 18 are disabled.

NOTE: See the *N8406-023 1Gb Intelligent L3 Switch Application Guide* for information on how to use port trunks.

The following table describes the Trunk Group Configuration commands.

Table 114 Trunk Group Configuration commands

| Command | Description |
|---|---|
| **portchannel** *<1-12>* **port** *<port number>* | Adds a physical port to the current trunk group.<br>**Command mode**: Global configuration |
| **no portchannel** *<1-12>* **port** *<port number>* | Removes a physical port from the current trunk group.<br>**Command mode**: Global configuration |
| **portchannel** *<1-12>* **enable** | Enables the current trunk group.<br>**Command mode**: Global configuration |
| **no portchannel** *<1-12>* **enable** | Disables the current trunk group.<br>**Command mode**: Global configuration |
| **no portchannel** *<1-12>* | Removes the current trunk group configuration.<br>**Command mode**: Global configuration |
| **show portchannel** *<1-12>* | Displays current trunk group parameters.<br>**Command mode**: All |

## Layer 2 IP Trunk Hash configuration

Trunk hash parameters are set globally for this switch. You can enable one or two parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SIP (source IP only)
- DIP (destination IP only)
- SIP + DIP (source IP and destination IP)
- SMAC + DMAC (source MAC and destination MAC)

The following table describes the IP Trunk Hash Configuration commands.

Table 115 IP Trunk Hash Set commands

| Command | Description |
|---|---|
| **portchannel hash source-mac-address** | Enable or disable trunk hashing on the source MAC.<br>**Command mode**: Global configuration |
| **portchannel hash destination-mac-address** | Enable or disable trunk hashing on the destination MAC.<br>**Command mode**: Global configuration |
| **portchannel hash source-ip-address** | Enable or disable trunk hashing on the source IP.<br>**Command mode**: Global configuration |
| **portchannel hash destination-ip-address** | Enable or disable trunk hashing on the destination IP.<br>**Command mode**: Global configuration |
| **portchannel hash source-destination-ip** | Enable trunk hashing on the source and destination IP.<br>**Command mode**: Global configuration |
| **portchannel hash source-destination-mac** | Enable trunk hashing on the source and destination MAC address.<br>**Command mode**: Global configuration |
| **show portchannel hash** | Display current trunk hash configuration.<br>**Command mode**: All |

# Link Aggregation Control Protocol configuration

The following table describes the LACP Configuration commands.

Table 116 LACP Configuration commands

| Command | Description |
|---|---|
| **lacp system-priority <***1-65535***>** | Defines the priority value (1 through 65535) for the switch. Lower numbers provide higher priority. The default value is 32768.<br>**Command mode**: Global configuration |
| **lacp timeout {short\|long}** | Defines the timeout period before invalidating LACP data from a remote partner. Choose **short** (3 seconds) or **long** (90 seconds). The default value is **long**.<br>**Command mode**: Global configuration |
| NOTE: We recommends that you use a timeout value of **long**, to reduce LACPDU processing. If your switch's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP. | |
| **show lacp** | Display current LACP configuration.<br>**Command mode**: All |

## LACP Port configuration

The following table describes the LACP Port Configuration commands.

Table 117 LACP Port Configuration commands

| Command | Description |
|---|---|
| **lacp mode {off\|active\|passive}** | Set the LACP mode for this port, as follows:<br>• **off**<br>Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is **off**.<br>• **active**<br>Turn LACP on and set this port to active. Active ports initiate LACPDUs.<br>• **passive**<br>Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports.<br>**Command mode**: Inerface port |
| **lacp priority <***1-65535***>** | Sets the priority value for the selected port. Lower numbers provide higher priority. Default is 32768.<br>**Command mode**: Inerface port |
| **lacp key <***1-65535***>** | Set the admin key for this port. Only ports with the same admin key and oper key (operational state generated internally) can form a LACP trunk group.<br>**Command mode**: Inerface port |
| **show interface gigabitethernet <***port number***> lacp** | Displays the current LACP configuration for this port.<br>**Command mode**: All |

# VLAN configuration

The commands in this section configure VLAN attributes, change the status of the VLAN, delete the VLAN, and change the port membership of the VLAN.

By default, the VLANs are disabled except VLAN 1 and 4095, which is always enabled. The switch supports a maximum of 1,000 VLANs. VLAN 4095 is reserved for switch management interface.

NOTE: See the *N8406-023 1Gb Intelligent L3 Switch Application Guide* for information on VLANs.

The following table describes the VLAN Configuration commands.

Table 118 VLAN Configuration commands

| Command | Description |
|---|---|
| **vlan** *<1-4095>* | Enter VLAN configuration mode.<br>**Command mode**: Global configuration |
| **name** *<1-32 characters>* | Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.<br>**Command mode**: VLAN configuration |
| **stg** *<0-128>* | Assigns a VLAN to a spanning tree group. STG number is assigned STGs 1-128 for STP/PVST+, only STG 1 for RSTP, and STGs 0-32 for MSTP (STG 0 is CIST).<br>**Command mode**: VLAN configuration |
| **member** *<port number>* | Adds ports to the VLAN membership.<br>**Command mode**: VLAN configuration |
| **no member** *<port number>* | Removes ports from the VLAN membership.<br>**Command mode**: VLAN configuration |
| **enable** | Enables this VLAN.<br>**Command mode**: VLAN configuration |
| **no enable** | Disables this VLAN without removing it from the configuration.<br>**Command mode**: VLAN configuration |
| **no vlan** *<1-4095>* | Deletes this VLAN.<br>**Command mode**: Global configuration |
| **show vlan** *<1-4095>* | Displays the current VLAN configuration.<br>**Command mode**: All |

IMPORTANT: All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on.

# Layer 3 configuration

The following table describes basic Layer 3 Configuration commands. The following sections provide more detailed information and commands. Layer 3 functionality is limited in this release.

Table 119 L3 Configuration commands

| Command | Description |
|---|---|
| **interface ip** *<1-256>* | Enter IP Interface mode.<br>**Command mode**: Global configuration |
| **route-map <***1-32***>** | Enter IP Route Map mode.<br>**Command mode**: Global configuration |
| **router rip** | Enter Router RIP mode.<br>**Command mode**: Global configuration |
| **router ospf** | Enter Router OSPF mode.<br>**Command mode**: Global configuration |
| **router vrrp** | Enter VRRP configuration mode.<br>**Command mode**: Global configuration |
| **ip router-id** *<IP address>* | Sets the router ID.<br>**Command mode**: Global configuration |
| **show layer3** | Displays the current IP configuration.<br>**Command mode**: All except User EXEC |

## IP interface configuration

The switch can be configured with up to 256 IP interfaces. Each IP interface represents the switch on an IP subnet on your network. The IP Interface option is disabled by default. Interface 256 is reserved for switch management.

The following table describes the IP Interface Configuration commands.

Table 120 IP Interface Configuration commands

| Command | Description |
|---|---|
| **interface ip** *<1-256>* | Enter IP interface mode.<br>**Command mode**: Global configuration |
| **ip address** *<IP address> <IP netmask>* | Configures the IP address and mask of the switch interface using dotted decimal notation.<br>**Command mode**: Interface IP |
| **[no] relay** | Enables or disables BOOTP relay on this IP interface. The default is enabled.<br>**Command mode**: Interface IP |
| **vlan** *<1-4094>* | Configures the VLAN number for this interface. Each interface can belong to one VLAN, though any VLAN can have multiple IP interfaces in it.<br>**Command mode**: Interface IP |
| **enable** | Enables this IP interface.<br>**Command mode**: Interface IP |
| **no enable** | Disables this IP interface.<br>**Command mode**: Interface IP |
| **no interface ip** *<1-256>* | Removes this IP interface.<br>**Command mode**: Global configuration |
| **show interface ip** *<1-256>* | Displays the current interface settings.<br>**Command mode**: All |

NOTE: If you enter an IP address for interface 1, you are prompted to change the BOOTP setting. Interface 256 is reserved for switch management interface.

## Default Gateway configuration

The switch supports up to four gateways. By default, no gateways are configured on the switch. Enter 1, 2, 3, or 4 in the command as the <*gateway instance*>, depending upon which gateway you want to configure. Gateway 4 is reserved for switch management.

The following table describes the Default IP Gateway Configuration commands.

Table 121 Default IP Gateway Configuration commands

| Command | Description |
|---|---|
| **ip gateway** <*1-4*> **address** <*IP address*> | Configures the IP address of the default IP gateway using dotted decimal notation.<br>**Command mode**: Global configuration |
| **ip gateway** <*1-4*> **interval** <*0-60*> | The switch pings the default gateway to verify that it is up. This option sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds.<br>**Command mode**: Global configuration |
| **ip gateway** <*1-4*> **retry** <*1-120*> | Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts.<br>**Command mode**: Global configuration |
| **[no] ip gateway** <*1-4*> **arp-health-check** | Enables or disables Address Resolution Protocol (ARP) health checks. This command is disabled by default.<br>**Command mode**: Global configuration |
| **ip gateway** <*1-4*> **enable** | Enables the gateway for use.<br>**Command mode**: Global configuration |
| **no ip gateway** <*1-4*> **enable** | Disables the gateway.<br>**Command mode**: Global configuration |
| **no ip gateway** <*1-4*> | Deletes the gateway from the configuration.<br>**Command mode**: Global configuration |
| **show ip gateway** <*1-4*> | Displays the current gateway settings.<br>**Command mode**: All except User EXEC |

NOTE: Gateway 4 is reserved for switch management interface.

# IP Static Route configuration

The following table describes the Static Route Configuration commands.

Table 122 Static Route Configuration commands

| Command | Description |
|---|---|
| **ip route <***IP subnet***> <***IP netmask***> <***IP nexthop***> <***IP interface (1-256)***>** | Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation.<br>**Command mode**: Global configuration |
| **no ip route <***IP subnet***> <***IP netmask***>** | Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation.<br>**Command mode**: Global configuration |
| **show ip route static** | Displays the current IPstatic route configuration.<br>**Command mode**: All except User Exec |

# Address Resolution Protocol configuration

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

The following table describes the ARP Configuration commands.

Table 123 ARP Configuration commands

| Command | Description |
|---|---|
| **ip arp rearp <***2-120***>** | Defines re-ARP period in minutes. You can set this duration between 2 and 120 minutes. The default is 10 minutes.<br>**Command mode**: Global configuration |
| **show ip arp** | Displays the current ARP configurations.<br>**Command mode:** All except User EXEC |

## Static ARP configuration

The following table describes the Static ARP Configuration commands.

Table 124 Static ARP Configuration commands

| Command | Description |
|---|---|
| **ip arp <***IP address***>** *<MAC address> <VLAN number> <port number>* | Adds a single ARP entry to switch memory.<br>**Command mode**: Global configuration |
| **no ip arp** *<IP address>* | Removes a single ARP entry from switch memory.<br>**Command mode**: Global configuration |
| **no ip arp all** | Clears the entire ARP list from switch memory.<br>**Command mode**: Global configuration |

# IP Forwarding configuration

The following table describes the IP Forwarding Configuration commands.

Table 125 IP Forwarding Configuration commands

| Command | Description |
|---|---|
| **[no] ip routing direct-broadcasts** | Enables or disables forwarding directed broadcasts. This command is disabled by default.<br>**Command mode**: Global configuration |
| **ip routing** | Enables IP forwarding (routing) on this switch.<br>**Command mode**: Global configuration |
| **no ip routing** | Disables IP forwarding (routing) on this switch. Forwarding is turned off by default.<br>**Command mode**: Global configuration |
| **show ip routing** | Displays the current IP forwarding settings.<br>**Command mode**: All except User EXEC |

# Network Filter configuration

The following table describes the Network Filter Configuration commands.

Table 126 Network Filter Configuration commands

| Command | Description |
|---|---|
| **ip match-address <***1-256***> <***IP address***> <***IP netmask***>** | Sets the starting IP address the IP subnet mask for this filter. The default address is 0.0.0.0<br>This command defines the range of IP addresses that will be accepted by the peer when the filter is enabled.<br>**Command mode**: Global configuration |
| **ip match-address <***1-256***> enable** | Enables the Network Filter configuration.<br>**Command mode**: Global configuration |
| **no ip match-address <***1-256***> enable** | Disables the Network Filter configuration.<br>**Command mode**: Global configuration |
| **no ip match-address <***1-256***>** | Deletes the Network Filter configuration.<br>**Command mode**: Global configuration |
| **show ip match-address [<***1-256***>]** | Displays the current the Network Filter configuration.<br>**Command mode**: All except User EXEC |

# Route Map configuration

Routing maps control and modify routing information. The *map number* (1-32) represents the routing map you wish to configure.

The following table describes the basic Route Map Configuration commands. The following sections provide more detailed information and commands.

Table 127 Route Map Configuration commands

| Command | Description |
|---|---|
| **route-map <***1-32***>** | Enter Route Map configuration mode.<br>**Command mode**: Global configuration |
| **[no] access-list <***1-8***>** | Configures the Access List.<br>**Command mode**: Route Map |
| **[no] metric <***1-16777214***>** | Sets the metric of the matched route.<br>**Command mode**: Route Map |
| **[no] metric-type {1\|2}** | Assigns the type of OSPF metric. The default is type 1.<br>• Type 1—External routes are calculated using both internal and external metrics.<br>• Type 2—External routes are calculated using only the external metrics.<br>• no—Removes the OSPF metric.<br>**Command mode**: Route Map |
| **precedence <***1-255***>** | Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10.<br>**Command mode**: Route Map |
| **enable** | Enables the route map.<br>**Command mode**: Route Map |
| **no enable** | Disables the route map.<br>**Command mode**: Route Map |
| **no route-map <***1-32***>** | Deletes the route map.<br>**Command mode**: Global configuration |
| **show route-map [<***1-32***>]** | Displays the current route configuration.<br>**Command mode**: All except User EXEC |

# IP Access List configuration

The *route map number* (1-32) and the *access list number* (1-8) represent the IP access list you wish to configure. The following table describes the IP Access List Configuration commands.

Table 128 IP Access List Configuration commands

| Command | Description |
|---|---|
| **[no] access-list <***1-8***> match-address <***1-256***>** | Sets the network filter number.<br>**Command mode**: Route Map |
| **[no] access-list <***1-8***> metric <***1-1677214***>** | Sets the metric value in the AS-External (ASE) LSA.<br>**Command mode**: Route Map |
| **access-list <***1-8***> action {permit\|deny}** | Permits or denies action for the access list.<br>**Command mode**: Route Map |
| **access-list <***1-8***> enable** | Enables the access list.<br>**Command mode**: Route Map |
| **no access-list <***1-8***> enable** | Disables the access list.<br>**Command mode:** Route Map |
| **no access-list <***1-8***>** | Deletes the access list.<br>**Command mode**: Route Map |
| **show route-map <***1-32***> access-list {<***1-8***>}** | Displays the current Access List configuration.<br>**Command mode**: All except User EXEC |

# Routing Information Protocol configuration

The RIP commands are used for configuring Routing Information Protocol parameters. This option is turned off by default.

The following table describes the basic RIP Configuration commands. The following section provides more detailed information and commands.

Table 129 RIP Configuration commands

| Command | Description |
|---|---|
| **router rip** | Enter router RIP configuration mode.<br>**Command mode**: Global configuration |
| **timers update <***1-120***>** | Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds.<br>**Command mod**e: Router RIP |
| **enable** | Globally turns RIP on.<br>**Command mode**: Router RIP |
| **no enable** | Globally turns RIP off. This is the default.<br>**Command mode**: Router RIP |
| **show ip rip** | Displays the current RIP configuration.<br>**Command mode**: All except User EXEC |

## RIP Interface configuration

The RIP commands are used for configuring Routing Information Protocol parameters. This option is turned off by default.

NOTE: Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

The following table describes the RIP Interface Configuration commands.

Table 130 RIP Interface Configuration commands

| Command | Description |
|---|---|
| **ip rip version {1\|2\|both}** | Configures the RIP version used by this interface. The default value is version 2.<br>**Command mode**: Interface IP |
| **[no] ip rip supply** | When enabled, the switch supplies routes to other routers. This command is enabled by default.<br>**Command mode**: Interface IP |
| **[no] ip rip listen** | When enabled, the switch learns routes from other routers. This command is enabled by default.<br>**Command mode**: Interface IP |
| **[no] ip rip poison** | When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. This command is disabled by default.<br>**Command mode**: Interface IP |
| **[no] ip rip split-horizon** | Enables or disables split horizon. The default value is enabled. |
| **[no] ip rip triggered** | Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message. The default value is enabled.<br>**Command mode**: Interface IP |
| **[no] ip rip multicast-updates** | Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is enabled.<br>**Command mode**: Interface IP |

Table 130 RIP Interface Configuration commands

| Command | Description |
|---|---|
| **[no] ip rip default-action {both\|listen\|supply}** | When listen, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. When supply, the switch sends RIP default routes to other routers. When both, the switch operates as both "listen" and "supply". When no, the switch rejects RIP default routes. This command is disabled by default.<br>**Command mode**: Interface IP |
| **ip rip metric <***1-15***>** | Configures the route metric, which indicates the relative distance to the destination. The default value is `1`.<br>**Command mode**: Interface IP |
| **[no] ip rip authentication type password** | Configures the authentication type. The default is `none`.<br>**Command mode**: Interface IP |
| **[no] ip rip authentication key <***password***>** | Configures the authentication key password.<br>**Command mod**e: Interface IP |
| **ip rip enable** | Enables this RIP interface.<br>**Command mode**: Interface IP |
| **no ip rip enable** | Disables this RIP interface. This is the default.<br>**Command mode**: Interface IP |
| **show interface ip <***1-256***> rip** | Displays the current RIP configuration.<br>**Command mode**: All except User EXEC |

## RIP Route Redistribution configuration

The following table describes the RIP Route Redistribute commands.

Table 131 RIP Redistribute commands

| Command | Description |
|---|---|
| **redistribute {fixed\|static\|ospf\|eospf} <***1-32***>** | Adds selected routing maps to the RIP route redistribution list. This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.<br>**Command mode**: Router RIP |
| **no redistribute {fixed\|static\|ospf\|eospf} <***1-32***>** | Removes the route map from the RIP route redistribution list.<br>**Command mode**: Router RIP |
| **[no] redistribute {fixed\|static\|ospf\|eospf} export {***metric* **<***1-15***>}** | Exports the routes of this protocol in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter `none`.<br>**Command mode**: Router RIP |
| **show ip rip redistribute** | Displays the current RIP route redistribute configuration.<br>**Command mode**: All except User EXEC |

# Open Shortest Path First configuration

The following table describes the basic Open Shortest Path First (OSPF) commands. The following sections provide more detailed information and commands.

Table 132 OSPF Configuration commands

| Command | Description |
|---|---|
| **router ospf** | Enter Router OSPF configuration mode.<br>**Command mode**: Router OSPF |
| **area <***0-2***>** | Configures the OSPF area.<br>**Command mode**: Router OSPF |
| **area-range <***1-16***>** | Configures the summary range.<br>**Command mode**: Router OSPF |
| **area-virtual-link <***1-3***>** | Configures a Virtual Link.<br>**Command mode**: Router OSPF |
| **message-digest-key <***1-255***> md5-key <***key string***>** | Assigns a string to MD5 authentication key.<br>**Command mode**: Router OSPF |
| **host <***1-128***>** | Configures an OSPF host route. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible.<br>**Command mode**: Router OSPF |
| **lsdb-limit <***0-2000***>** | Sets the link state database limit. The default value is 0.<br>**Command mode**: Router OSPF |
| **[no] default-information <***1-16777214***> {1\|2}** | Sets one default route among multiple choices in an area.<br>**Command mode**: Router OSPF |
| **enable** | Enables OSPF.<br>**Command mode**: Router OSPF |
| **no enable** | Disables OSPF. This is the default.<br>**Command mode**: Router OSPF |
| **show ip ospf** | Displays the current OSPF configuration settings.<br>**Command mode**: All except User EXEC |

# OSFP Area Index configuration

The following table describes the Area Index Configuration commands.

Table 133 OSPF Area Index Configuration commands

| Command | Description |
|---|---|
| **area <*0-2*> area-id <*A.B.C.D*>** | Defines the area ID of the OSPF area number.<br>**Command mode**: Router OSPF |
| **area <*0-2*> type {transit\|stub\|nssa}** | Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.<br>• **Transit area:** allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.<br>• **Stub area:** is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.<br>• **NSSA:** Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.<br>The default is transit.<br>**Command mode**: Router OSPF |
| **area <*0-2*> stub-metric <*1-65535*>** | Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions.<br>Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes. The default value is 1.<br>**Command mode**: Router OSPF |
| **[no] area <*0-2*> authentication-type {password\|md5}** | Defines the authentication method, as follows:<br>• **No:** No authentication required.<br>• **Password:** Authenticates simple passwords so that only trusted routing devices can participate.<br>• **MD5:** This parameter is used when MD5 cryptographic authentication is required.<br>The default is none.<br>**Command mode**: Router OSPF |
| **area <*0-2*> spf-interval <*1-255*>** | Sets time interval between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm.The default value is 10.<br>**Command mode**: Router OSPF |
| **area <*0-2*> enable** | Enables the OSPF area.<br>**Command mode**: Router OSPF |
| **no area <*0-2*> enable** | Disables the OSPF area. This is the default.<br>**Command mode**: Router OSPF |
| **no area <*0-2*>** | Deletes the OSPF area.<br>**Command mode**: Router OSPF |
| **show ip ospf area <*0-2*>** | Displays the current OSPF configuration.<br>**Command mode**: All except User EXEC |

## OSPF Summary Range configuration

The following table describes the OSPF Summary Range Configuration commands.

Table 134 OSPF Summary Range Configuration commands

| Command | Description |
|---|---|
| **area-range <***1-16***> address <***IP address***> <***IP netmask***>** | Configures the base IP address and IP address mask for the range.<br>**Command mode**: Router OSPF |
| **area-range <***1-16***> area <***0-2***>** | Configures the area index used by the switch. The default is 0.<br>**Command mode**: Router OSPF |
| **[no] area-range <***1-16***> hide** | Hides the OSPF summary range. The default is none.<br>**Command mode**: Router OSPF |
| **area-range <***1-16***> enable** | Enables the OSPF summary range.<br>**Command mode**: Router OSPF |
| **no area-range <***1-16***> enable** | Disables the OSPF summary range. This is the default.<br>**Command mode**: Router OSPF |
| **no area-range <***1-16***>** | Deletes the OSPF summary range.<br>**Command mode**: Router OSPF |
| **show ip ospf area-range <***1-16***>** | Displays the current OSPF summary range.<br>**Command mode**: All except User EXEC |

## OSPF Interface configuration

The following table describes the OSPF Interface Configuration commands.

Table 135 OSPF Interface Configuration commands

| Command | Description |
|---|---|
| **ip ospf area <***0-2***>** | Configures the OSPF area index.<br>**Command mode**: Interface IP |
| **ip ospf priority <***0-255***>** | Configures the assigned priority value to the OSPF interfaces.<br>(A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR). The default value is 1.<br>**Command mode**: Interface IP |
| **ip ospf cost <***1-65535***>** | Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth. The default value is 1.<br>**Command mode**: Interface IP |
| **ip ospf hello-interval <***1-65535***>** | Configures the interval in seconds between the `hello` packets for the interfaces. The default is 10 seconds.<br>**Command mode**: Interface IP |
| **ip ospf dead-interval <***1-65535***>** | Configures the health parameters of a `hello` packet, which is set for an interval of seconds before declaring a silent router to be down. The default is 40 seconds.<br>**Command mode**: Interface IP |
| **ip ospf transit-delay <***1-3600***>** | Configures the transit delay in seconds. The default is 1 second.<br>**Command mode**: Interface IP |
| **ip ospf retransmit-interval <***1-3600***>** | Configures the retransmit interval in seconds. The default is 5 seconds.<br>**Command mode**: Interface IP |
| **[no] ip ospf key <***key string***>** | Sets the authentication key to clear the password.<br>**Command mode**: Interface IP |
| **[no] ip ospf message-digest-key <***1-255***>** | Assigns an MD5 key to the interface. The default is none.<br>**Command mode**: Interface IP |
| **ip ospf enable** | Enables the OSPF interface.<br>**Command mode**: Interface IP |

Table 135 OSPF Interface Configuration commands

| Command | Description |
|---|---|
| **no ip ospf enable** | Disables the OSPF interface. The default is disabled.<br>**Command mode**: Interface IP |
| **no ip ospf** | Deletes the OSPF interface.<br>**Command mode**: Interface IP |
| **show interface ip <***1-256***> ospf** | Displays the current settings for OSPF interface.<br>**Command mode**: All |

## OSPF Virtual Link configuration

The following table describes the OSPF Virtual Link Configuration commands.

Table 136 OSPF Virtual Link Configuration commands

| Command | Description |
|---|---|
| **area-virtual-link <***1-3***> area <***0-2***>** | Configures the OSPF area index. The default is 0.<br>**Command mode**: Router OSPF |
| **area-virtual-link <***1-3***> hello-interval <***1-65535***>** | Configures the authentication parameters of a hello packet, which is set to be in an interval of seconds. The default is 10 seconds.<br>**Command mode**: Router OSPF |
| **area-virtual-link <***1-3***> dead-interval <***1-65535***>** | Configures the health parameters of a hello packet, which is set to be in an interval of seconds. Default is 60 seconds.<br>**Command mode**: Router OSPF |
| **area-virtual-link <***1-3***> transit-delay <***1-3600***>** | Configures the delay in transit in seconds. Default is one second.<br>**Command mode**: Router OSPF |
| **area-virtual-link <***1-3***> retransmit-interval <***1-3600***>** | Configures the retransmit interval in seconds. Default is five seconds.<br>**Command mode**: Router OSPF |
| **area-virtual-link <***1-3***> neighbor-router <***IP address***>** | Configures the router ID of the virtual neighbor. Default is 0.0.0.0<br>**Command mode**: Router OSPF |
| **[no] area-virtual-link <***1-3***> key <***key string***>** | Configures the password (up to eight characters) for each virtual link. Default is `none`.<br>**Command mode**: Router OSPF |
| **[no] area-virtual-link <***1-3***> message-digest-key <***1-255***>** | Sets MD5 key ID for each virtual link. Default is `none`.<br>**Command mode**: Router OSPF |
| **area-virtual-link <***1-3***> enable** | Enables OSPF virtual link.<br>**Command mode**: Router OSPF |
| **no area-virtual-link <***1-3***> enable** | Disables OSPF virtual link. This is the default.<br>**Command mode**: Router OSPF |
| **no area-virtual-link <***1-3***>** | Deletes OSPF virtual link.<br>**Command mode**: Router OSPF |
| **show ip ospf area-virtual-link <***1-3***>** | Displays the current OSPF virtual link settings.<br>**Command mode**: All except User EXEC |

## OSPF Host Entry configuration

The following table describes the OSPF Host Entry Configuration commands.

Table 137 OSPF Host Entry Configuration commands

| Command | Description |
|---|---|
| **host <***1-128***> address <***IP address***>** | Configures the base IP address for the host entry.<br>**Command mode**: Router OSPF |
| **host <***1-128***> area <***0-2***>** | Configures the area index of the host. The default is 0.<br>**Command mode**: Router OSPF |

Table 137 OSPF Host Entry Configuration commands

| Command | Description |
|---|---|
| **host <***1-128***> cost <***1-65535***>** | Configures the cost value of the host. The default value is 1.<br>**Command mode**: Router OSPF |
| **host <***1-128***> enable** | Enables OSPF host entry.<br>**Command mode**: Router OSPF |
| **no host <***1-128***> enable** | Disables OSPF host entry. This is the default.<br>**Command mode**: Router OSPF |
| **no host <***1-128***>** | Deletes OSPF host entry.<br>**Command mode**: Router OSPF |
| **show ip ospf host <***1-128***>** | Displays the current OSPF host entries.<br>**Command mode**: All except User EXEC |

## OSPF Route Redistribution configuration

The following table describes the OSPF Route Redistribution Configuration commands.

Table 138 OSPF Route Redistribution Configuration commands

| Command | Description |
|---|---|
| **redistribute {fixed\|static\|rip} <***1-32***>** | Adds selected routing maps to the rmap list.<br>This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.<br>**Command mode**: Router OSPF |
| **no redistribute {fixed\|static\|rip} <***1-32***>** | Removes the route map from the route redistribution list.<br>Removes routing maps from the `rmap` list.<br>**Command mode**: Router OSPF |
| **[no] redistribute {fixed\|static\|rip} export** *metric* **<***1-16777214***>** *metric-type* **{1\|2}** | Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified.<br>**Command mode**: Router OSPF |
| **show ip ospf redistribute** | Displays the current route map settings.<br>**Command mode**: All except User EXEC |

## OSPF MD5 Key configuration

The following table describes the OSPF MD5 Key Configuration commands.

Table 139 OSPF MD5 Key Configuration commands

| Command | Description |
|---|---|
| **message-digest-key <***1-255***> md5-key <***key string***>** | Sets the authentication key up to 16 characters for this OSPF packet.<br>**Command mode**: Router OSPF |
| **no message-digest-key <***1-255***>** | Deletes the authentication key for this OSPF packet.<br>**Command mode**: Router OSPF |
| **show ip ospf message-digest-key <***1-255***>** | Displays the current MD5 key configuration.<br>**Command mode**: All except User EXEC |

# IGMP configuration

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

## IGMP snooping configuration

The following table describes the IGMP Snooping Configuration commands.

Table 140 IGMP Snooping commands

| Command | Description |
|---|---|
| **ip igmp snoop timeout** *<1-255>* | Sets the Maximum Response Time (MRT) for IGMP hosts. MRT is one of the parameters used to determine the age out period of the IGMP hosts. Increasing the timeout increases the age out period.<br>The range is from 1 to 255 seconds. The default is 10 seconds.<br>**Command mode:** Global configuration |
| **ip igmp snoop mrouter-timeout** *<1-600>* | Configures the age-out period for the IGMP Mrouters in the Mrouter table. If the switch does not receive a General Query from the Mrouter for `mrto` seconds, the switch removes the multicast router from its Mrouter table.<br>The range is from 1 to 600 seconds. The default is 255 seconds.<br>**Command mode:** Global configuration |
| **ip igmp snoop query-interval** *<1-600>* | Sets the IGMP router query interval. The range is 1-600 seconds. The default value is 125.<br>**Command mode:** Global configuration |
| **ip igmp snoop robust** *<2-10>* | Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), then increase the value. The default value is 2.<br>**Command mode:** Global configuration |
| **[no] ip igmp snoop aggregate** | Enables or disables IGMP Membership Report aggregation. The default is enabled.<br>**Command mode:** Global configuration |
| **ip igmp snoop source-ip** *<IP address>* | Configures the source IP address used as a proxy for IGMP Group Specific Queries.<br>**Command mode:** Global configuration |
| **ip igmp snoop vlan** *<1-4094>* | Adds the VLAN to IGMP Snooping.<br>**Command mode:** Global configuration |
| **no ip igmp snoop vlan** *<1-4094>* | Removes the VLAN from IGMP Snooping.<br>**Command mode:** Global configuration |
| **no ip igmp snoop vlan all** | Removes all VLANs from IGMP Snooping.<br>**Command mode:** Global configuration |
| **[no] ip igmp snoop vlan** *<1-4094>* **fast-leave** | Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is disabled by default.<br>**Command mode:** Global configuration |
| **ip igmp snoop enable** | Enables IGMP Snooping.<br>**Command mode:** Global configuration |
| **no ip igmp snoop enable** | Disables IGMP Snooping. This is the default.<br>**Command mode:** Global configuration |
| **show ip igmp snoop** | Displays the current IGMP Snooping parameters.<br>**Command mode:** All except User EXEC |

## IGMP static multicast router configuration

The following table describes the Static Multicast Router Configuration commands.

NOTE: When you configure a static multicast router on a VLAN, the process of learning multicast routers is disabled for that VLAN.

Table 141 IGMP Static Multicast Router commands

| Command | Description |
|---|---|
| **ip igmp mrouter** <*port number*> <*1-4094*> <*1-2*> | Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1 or 2) of the multicast router.<br>**Command mode:** Global configuration |
| **no ip igmp mrouter** <*port number*> <*1-4094*> <*1-2*> | Removes a static multicast router from the selected port/VLAN combination.<br>**Command mode:** Global configuration |
| **show ip igmp mrouter** | Displays the current IGMP Static Multicast Router parameters.<br>**Command mode:** All except User EXEC |

## IGMP filtering configuration

The following table describes the IGMP Filter Configuration commands.

Table 142 IGMP Filtering commands

| Command | Description |
|---|---|
| **ip igmp filtering** | Enables IGMP filtering globally.<br>**Command mode:** Global configuration |
| **no ip igmp filtering** | Disables IGMP Filtering globally. This is the default.<br>**Command mode:** Global configuration |
| **show ip igmp filtering** | Displays the current IGMP Filtering parameters.<br>**Command mode:** All except User EXEC |

## IGMP filter definition

The following table describes the IGMP Filter Definition commands.

Table 143 IGMP Filter Definition commands

| Command | Description |
|---|---|
| **ip igmp profile** <*1-16*> **range** <*IP multicast address*> <*IP multicast address*> | Configures the range of IP multicast addresses for this filter. Enter the first IP multicast address of the ranger, followed by the second IP multicast address of the range.<br>**Command mode:** Global configuration |
| **ip igmp profile** <*1-16*> **action {allow\|deny}** | Allows or denies multicast traffic for the IP multicast addresses specified.<br>**Command mode:** Global configuration |
| **ip igmp profile** <*1-16*> **enable** | Enables this IGMP filter.<br>**Command mode:** Global configuration |
| **no ip igmp profile** <*1-16*> **enable** | Disables this IGMP filter. This is the default.<br>**Command mode:** Global configuration |
| **no ip igmp profile** <*1-16*> | Deletes this filter's parameter definitions.<br>**Command mode:** Global configuration |
| **show ip igmp profile** <*1-16*> | Displays the current IGMP filter.<br>**Command mode:** All except User EXEC |

## IGMP filtering port configuration

The following table describes the IGMP Port Filtering Configuration commands.

Table 144 IGMP Filtering Port commands

| Command | Description |
|---|---|
| **[no] ip igmp filtering** | Enables or disables IGMP Filtering on this port. The default is disabled.<br>**Command mode:** Interface port |
| **ip igmp profile** *<1-16>* | Adds an IGMP filter to this port.<br>**Command mode:** Interface port |
| **no ip igmp profile** *<1-16>* | Removes an IGMP filter from this port.<br>**Command mode:** Interface port |
| **show interface gigabitethernet** *<port number>* **igmp-filtering** | Displays the current IGMP filter parameters for this port.<br>**Command mode:** All |

# Domain Name System configuration

The Domain Name System (DNS) Configuration commands are used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the ping, traceroute, and tftp commands.

The following table describes the Domain Name System (DNS) Configuration commands.

Table 145 Domain Name System (DNS) Configuration commands

| Command | Description |
|---|---|
| **[no] ip dns primary-server** *<IP address>* | Sets the IP address for your primary DNS server. Use dotted decimal notation.<br>**Command mode:** Global configuration |
| **[no] ip dns secondary-server** *<IP address>* | Sets the IP address for your secondary DNS server. If the primary DNS server fails, the configured secondary will be used instead. Enter the IP address using dotted decimal notation.<br>**Command mode:** Global configuration |
| **[no] ip dns domain-name** *<string>* | Sets the default domain name used by the switch.<br>For example: `mycompany.com`<br>**Command mode:** Global configuration |
| **show ip dns** | Displays the current Domain Name System (DNS) settings.<br>**Command mode:** All except User EXEC |

# Bootstrap Protocol Relay configuration

Bootstrap Protocol (BOOTP) Relay is used to allow hosts to obtain their configurations from a Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to two DHCP/BOOTP servers with IP addresses that have been configured on this switch.

BOOTP relay is turned off by default.

The following table describes the BOOTP Configuration commands.

Table 146 BOOTP Configuration commands

| Command | Description |
|---|---|
| **[no] ip bootp-relay {server1\|server2} <***IP address***>** | Sets the IP address of the first or second BOOTP server.<br>**Command mode**: Global configuration |
| **ip bootp-relay enable** | Globally turns on BOOTP relay.<br>**Command mode**: Global configuration |
| **no ip bootp-relay enable** | Globally turns on BOOTP relay. This is the default.<br>**Command mode**: Global configuration |
| **show ip bootp-relay** | Displays the current BOOTP relay configuration.<br>**Command mode**: All except User EXEC |

# Virtual Router Redundancy Protocol configuration

Virtual Router Redundancy Protocol (VRRP) support on this switch provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

By default, VRRP is disabled. For more information on VRRP, see the “High Availability” chapter in the *N8406-023 1Gb Intelligent L3 Switch Application Guide*.

The following table describes the basic VRRP Configuration commands. The following sections provide more detailed information and commands.

Table 147 VRRP Configuration commands

| Command | Description |
|---|---|
| **router vrrp** | Enter VRRP configuration mode.<br>**Command mode:** Router VRRP |
| **enable** | Globally enables VRRP on this switch.<br>**Command mode:** Router VRRP |
| **no enable** | Globally disables VRRP on this switch. This is the default.<br>**Command mode:** Router VRRP |
| **show ip vrrp** | Displays the current VRRP parameters.<br>**Command mode:** All except User EXEC |

## VRRP Virtual Router configuration

Virtual Router commands are used for configuring up to 255 virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Virtual routers are disabled by default.

The following table describes the Virtual Router Configuration commands.

Table 148 Virtual Router Configuration commands

| Command | Description |
|---|---|
| **virtual-router <***1-255***>**<br>**virtual-router-id <***1-255***>** | Defines the virtual router ID. This is used in conjunction with `addr` (below) to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router: one that shares the same `virtual router ID` and `address` combination.<br>The `vrid` for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. The default value is 1.<br>All `virtual router ID` values must be unique within the VLAN to which the virtual router’s IP interface belongs.<br>**Command mode:** Router VRRP |
| **virtual-router <***1-255***>**<br>**address <***IP address***>** | Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the `vrid` (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0<br>**Command mode:** Router VRRP |

Table 148 Virtual Router Configuration commands

| Command | Description |
|---|---|
| **virtual-router <*1-255*> interface <*1-255*>** | Selects a switch IP interface (between 1 and 255). If the IP interface has the same IP address as the `address` option above, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must preempt another virtual router which has assumed master routing authority. This preemption occurs even if the `preemption` option below is disabled. The default value is 1.<br>**Command mode:** Router VRRP |
| **virtual-router <*1-255*> priority <*1-254*>** | Defines the election priority bias for this virtual server. This can be any integer between 1 and 254. The default value is 100.<br>During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).<br>When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.<br>**Command mode:** Router VRRP |
| **virtual-router <*1-255*> timers advertise <*1-255*>** | Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is 1.<br>**Command mode:** Router VRRP |
| **[no] virtual-router <*1-255*> preemption** | Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preemption` is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router `address` are the same). By default, this option is enabled. |
| **virtual-router <*1-255*> enable** | Enables this virtual router.<br>**Command mode:** Router VRRP |
| **no virtual-router <*1-255*> enable** | Disables this virtual router. This is the default.<br>**Command mode:** Router VRRP |
| **no virtual-router <*1-255*>** | Deletes this virtual router from the switch configuration.<br>**Command mode:** Router VRRP |
| **show ip vrrp virtual-router <*1-255*>** | Displays the current configuration information for this virtual router.<br>**Command mode:** All except User EXEC |

# VRRP Virtual Router Priority Tracking configuration

These commands are used to modify the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through VRRP Tracking.

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria (`virtual routers`, `interfaces`, and `ports` below) apply to standard virtual routers, otherwise called “virtual interface routers”. A *virtual server* router is defined as any virtual router whose IP address is the same as any configured virtual server IP address.

The following table describes the Virtual Router Priority Tracking Configuration commands.

Table 149 Virtual Router Priority Tracking Configuration commands

| Command | Description |
|---|---|
| **[no] virtual-router <***1-255***> track virtual-routers** | When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.<br>**Command mode:** Router VRRP |
| **[no] virtual-router <***1-255***> track interfaces** | When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.<br>**Command mode:** Router VRRP |
| **[no] virtual-router <***1-255***> track ports** | When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.<br>**Command mode:** Router VRRP |
| **show ip vrrp virtual-router <***1-255***> track** | Displays the current configuration for priority tracking for this virtual router.<br>**Command mode:** All except User EXEC |

# VRRP Virtual Router Group configuration

The Virtual Router Group commands are used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the switch to either be master or backup as a group. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

The following table describes the Virtual Router Group Configuration commands.

Table 150 Virtual Router Group Configuration commands

| Command | Description |
|---|---|
| **group virtual-router-id <***1-255***>** | Defines the virtual router ID.<br>The `virtual router ID` for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. All `virtual router ID` values must be unique within the VLAN to which the virtual router’s IP interface belongs. The default virtual router ID is 1.<br>**Command mode:** Router VRRP |
| **group interface <***1-255***>** | Selects a switch IP interface. The default switch IP interface number is 1.<br>**Command mode:** Router VRRP |

Table 150 Virtual Router Group Configuration commands

| Command | Description |
|---|---|
| **group priority <***1-254***>** | Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100.<br>During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).<br>When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.<br>**Command mode:** Router VRRP |
| **group advertisement <***1-255***>** | Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.<br>**Command mode:** Router VRRP |
| **[no] group preemption** | Enables or disables master preemption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preemption` is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router `address` are the same). By default, this option is enabled.<br>**Command mode:** Router VRRP |
| **group enable** | Enables the virtual router group.<br>**Command mode:** Router VRRP |
| **no group enable** | Disables the virtual router group. This is the default.<br>**Command mode:** Router VRRP |
| **no group** | Deletes the virtual router group from the switch configuration.<br>**Command mode:** Router VRRP |
| **show ip vrrp group** | Displays the current configuration information for the virtual router group.<br>**Command mode:** All except User EXEC |

## VRRP Virtual Router Group Priority Tracking configuration

The following table describes the Virtual Router Group Priority Tracking Configuration commands.

Table 151 Virtual Router Group Priority Tracking Configuration commands

| Command | Description |
|---|---|
| **[no] group track interfaces** | When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.<br>**Command mode:** Router VRRP |
| **[no] group track ports** | When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered "active" if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.<br>**Command mode:** Router VRRP |
| **show ip vrrp group track** | Displays the current configuration for priority tracking for this virtual router.<br>**Command mode:** All except User EXEC |

NOTE: If *Virtual Router Group Tracking* is enabled, then the tracking option will be available only under *group* option. The tracking setting for the other individual virtual routers is ignored.

## VRRP Interface configuration

These commands are used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers. The *interface-number* represents the IP interface on which authentication parameters must be configured.

The following table describes the VRRP Interface Configuration commands.

Table 152 VRRP Interface Configuration commands

| Command | Description |
|---|---|
| **interface <***1-255***> authentication {password\|none}** | Defines the type of authentication that will be used: `none` (no authentication), or `password` (password authentication). The default is none.<br>**Command mode:** Router VRRP |
| **interface <***1-255***> password {<***password***>\|none}** | Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen.<br>**Command mode:** Router VRRP |
| **no interface <***1-255***>** | Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted.<br>**Command mode:** Router VRRP |
| **show ip vrrp interface <***1-255***>** | Displays the current configuration for this IP interface's authentication parameters.<br>**Command mode:** All except User EXEC |

## VRRP Tracking configuration

These commands are used for setting weights for the various criteria used to modify priority levels during the master router election process. Each time one of the tracking criteria is met, the priority level for the virtual router is increased.

The following table describes the VRRP Tracking Configuration commands.

Table 153 VRRP Tracking Configuration commands

| Command | Description |
|---|---|
| **tracking-priority-increment virtual-routers <***0-254***>** | Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2.<br>**Command mode:** Router VRRP |
| **tracking-priority-increment interfaces <***0-254***>** | Defines the priority increment value (0 through 254) for active IP interfaces detected on this switch. The default value is 2.<br>**Command mode:** Router VRRP |
| **tracking-priority-increment ports <***0-254***>** | Defines the priority increment value (0 through 254) for active ports on the virtual router's VLAN. The default value is 2.<br>**Command mode:** Router VRRP |
| **show ip vrrp tracking-priority-increment** | Displays the current configuration of priority tracking increment values.<br>**Command mode:** All except User EXEC |

NOTE: These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under VRRP Virtual Router Priority Tracking are enabled.

# Quality of Service configuration

Use the Quality of Service (QoS) commands to configure the IEEE 802.1p priority value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

## QoS 802.1p configuration

This feature provides the switch the capability to filter IP packets based on the IEEE 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority bits are given forwarding preference over packets with numerically lower priority bits value.

The following table describes the 802.1p Configuration commands.

Table 154 802.1p Configuration commands

| Command | Description |
|---|---|
| **qos transmit-queue mapping <***priority (0-7)***> <***queue (0-1)***>** | Maps the 802.1p priority to the Class of Service queue (COSq). Enter the 802.1p priority value (0-7), followed by the Class of Service queue (0-1) that handles the matching traffic.<br>**Command mode:** Global configuration |
| **qos transmit-queue weight-cos <***queue (0-1)***> <***weight (0-15)***>** | Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-1), followed by the scheduling weight (0-15).<br>**Command mode:** Global configuration |
| **show qos transmit-queue** | Displays the current 802.1p parameters.<br>**Command mode:** All |
| **show qos transmit-queue information** | Displays the current 802.1p parameters, and the 802.1p priority level for each port.<br>**Command mode:** All |

# Access Control configuration

Use these commands to create Access Control Lists (ACLs) and ACL Groups. ACLs define matching criteria used for IP filtering and Quality of Service functions.

## Access Control List configuration

These commands allow you to define filtering criteria for each Access Control List (ACL). The following table describes the basic ACL Configuration commands.

Table 155 ACL Configuration commands

| Command | Description |
|---|---|
| **[no] access-control list <***ACL number***> egress-port <***port number***>** | Configures the ACL to function on egress packets.<br>The egress port ACL will not match a Layer 2 broadcast or multicast packet. The egress port ACL will not match packets if the destination port is a trunk.<br>**Command mode:** Global configuration |
| **access-control list <***ACL number***> action {permit\|deny\|set-priority <***0-7***>}** | Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the Class of Service queue that handles the packets.<br>**Command mode:** Global configuration |
| **access-control list <***ACL number***> statistics** | Enables or disables the statistics collection for the Access Control List. The default is disabled.<br>**Command mode:** Global configuration |
| **default access-control list <***ACL number***>** | Resets the ACL parameters to their default values.<br>**Command mode:** Global configuration |
| **show access-control list <***ACL number***>** | Displays the current ACL parameters.<br>**Command mode:** All |

NOTE: ACL number is available from 1 to 762. ACLs are divided into Precedence Groups. Each Precedence Group provides a different set of packet classifiers for the ACLs within the Precedence Group. See the "Quality of Service" chapter in the *Application Guide*.

## ACL Ethernet Filter configuration

These commands allow you to define Ethernet matching criteria for an ACL. The following table describes the Ethernet Filter Configuration commands.

Table 156 Ethernet Filter Configuration commands

| Command | Description |
|---|---|
| **[no] access-control list <***ACL number***> ethernet source-mac-address <***MAC address***> [<***MAC mask***>]** | Defines the source MAC address and MAC mask for this ACL. For example:<br>00:60:cf:40:56:00 ff:ff:ff:ff:ff:fc<br>**Command mode:** Global configuration |
| **[no] access-control list <***ACL number***> ethernet destination-mac-address <***MAC address***> [<***MAC mask***>]** | Defines the destination MAC address and MAC mask for this ACL. For example:<br>00:60:cf:40:56:00 ff:ff:ff:ff:ff:fc<br>**Command mode:** Global configuration |
| **[no] access-control list <***ACL number***> ethernet vlan <***1-4095***> [<***mask***>]** | Defines a VLAN number and mask for this ACL.<br>**Command mode:** Global configuration |
| **[no] access-control list <***ACL number***> ethernet ethernet-type {arp\|ip\|ipv6\|mpls\|rarp\|any\|0xXXXX}** | Defines the Ethernet type for this ACL.<br>**Command mode:** Global configuration |
| **[no] access-control list <***ACL number***> ethernet priority <***0-7***>** | Defines the Ethernet priority value for the ACL.<br>**Command mode:** Global configuration |

Table 156 Ethernet Filter Configuration commands

| Command | Description |
|---|---|
| **default access-control list <***ACL number***> ethernet** | Resets Ethernet parameters for the ACL to their default values.<br>**Command mode:** Global configuration |
| **show access-control list <***ACL number***> ethernet** | Displays the current Ethernet parameters for the ACL.<br>**Command mode:** All |

## ACL IP Version 4 Filter configuration

These commands allow you to define IPv4 matching criteria for an ACL. The following table describes the IP version 4 Filter Configuration commands.

Table 157 IPv4 Filter Configuration commands

| Command | Description |
|---|---|
| **[no] access-control list <***ACL number***> ipv4 source-ip-address <***IP address***> [<***IP mask***>]** | Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.<br>**Command mode:** Global configuration |
| **[no] access-control list <***ACL number***> ipv4 destination-ip-address <***IP address***> [<***IP mask***>]** | Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.<br>**Command mode:** Global configuration |
| **[no] access-control list <***ACL number***> ipv4 protocol <***0-255***>** | Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols.<br>Number Name<br>1 icmp<br>2 igmp<br>6 tcp<br>17 udp<br>89 ospf<br>112 vrrp<br>**Command mode:** Global configuration |
| **[no] access-control list <***ACL number***> ipv4 type-of-service <***0-255***>** | Defines a Type of Service value for the ACL. For more information on ToS, see RFC 1340 and 1349.<br>**Command mode:** Global configuration |
| **default access-control list <***ACL number***> ipv4** | Resets the IPv4 parameters for the ACL to their default values.<br>**Command mode:** Global configuration |
| **show access-control list <***ACL number***> ipv4** | Displays the current IPV4 parameters.<br>**Command mode:** All |

# ACL TCP/UDP Filter configuration

These commands allow you to define TCP/UDP matching criteria for an ACL. The following table describes the TCP/UDP Filter Configuration commands.

Table 158 TCP/UDP Filter Configuration commands

| Command | Description |
|---|---|
| **[no] access-control list <***ACL number***> tcp-udp source-port <***1-65535***> [<***port mask***>]** | Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports:<br>Number Name<br>20 ftp-data<br>21 ftp<br>22 ssh<br>23 telnet<br>25 smtp<br>37 time<br>42 name<br>43 whois<br>53 domain<br>69 tftp<br>70 gopher<br>79 finger<br>80 http<br>**Command mode:** Global configuration |
| **[no] access-control list <***ACL number***> tcp-udp destination-port <***1-65535***> [<***port mask***>]** | Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with `source-port` above.<br>**Command mode:** Global configuration |
| **[no] access-control list <***ACL number***> tcp-udp flags <***value (0x0-0x3f)***> [<***mask***>]** | Defines a TCP/UDP flag for the ACL.<br>**Command mode:** Global configuration |
| **default access-control list <***ACL number***> tcp-udp** | Resets the TCP/UDP parameters for the ACL to their default values.<br>**Command mode:** Global configuration |
| **show access-control list <***ACL number***> tcp-udp** | Displays the current TCP/UDP Filtering parameters.<br>**Command mode:** All |

# ACL Packet Format configuration

The following table describes the Packet Format Configuration commands.

Table 159 Packet Format Configuration commands

| Command | Description |
|---|---|
| **[no] access-control list <***ACL number***> packet-format ethernet {ethernet-type2\|snap\|llc}** | Defines the Ethernet format for the ACL. The default is none.<br>**Command mode:** Global configuration |
| **[no] access-control list <***ACL number***> packet-format tagged** | Defines the tagging format for the ACL. The default is none.<br>**Command mode:** Global configuration |
| **default access-control list <***ACL number***> packet-format** | Resets Packet Format parameters for the ACL to their default values.<br>**Command mode:** Global configuration |
| **show access-control list <***ACL number***> packet-format** | Displays the current Packet Format parameters for the ACL.<br>**Command mode:** All |

## ACL Metering configuration

The following table describes the ACL Metering Configuration commands.

Table 160 ACL Metering Configuration commands

| Command | Description |
|---|---|
| **access-control list <***ACL number***> meter committed-rate <***64–1000000***>** | Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64. The default is 64.<br>**Command mode**: Global configuration |
| **access-control list <***ACL number***> meter maximum-burst-size <***32–4096***>** | Configures the maximum burst size, in Kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096<br>The default is 32.<br>**Command mode**: Global configuration |
| **[no] access-control list <***ACL number***> meter enable** | Enables or disables Metering on the ACL. The default is disabled.<br>**Command mode**: Global configuration |
| **access-control list <***ACL number***> meter action {drop\|pass}** | Configures the ACL Meter to either drop or pass out-of-profile traffic.<br>**Command mode**: Global configuration |
| **default access-control list <***ACL number***> meter** | Reset ACL Metering parameters to their default values.<br>**Command mode**: Global configuration |
| **show access-control list <***ACL number***> meter** | Displays the current ACL metering parameters.<br>**Command mode**: All |

## ACL Re-mark configuration

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within the ACL Metering profile, or out of the ACL Metering profile.

The following table describes the ACL Re-mark Configuration commands.

Table 161 ACL Re-mark Configuration commands

| Command | Description |
|---|---|
| **[no] access-control list <***ACL number***> re-mark** | Assign an ACL for DSCP Re-marking.<br>**Command mode**: Global configuration |
| **default access-control list <***ACL number***> re-mark** | Reset ACL Re-mark parameters to their default values.<br>**Command mode**: Global configuration |
| **show access-control list <***ACL number***> re-mark** | Displays the current ACL re-mark parameters.<br>**Command mode**: All |

## ACL Re-mark In-Profile configuration

The following table describes the ACL Re-mark In-Profile Configuration commands.

Table 162 ACL Re-mark In-Profile Configuration commands

| Command | Description |
|---|---|
| **[no] access-control list <***ACL number***> re-mark in-profile dscp <***0–63***>** | Sets the DiffServ Code Point (DSCP) of In-Profile packets to the selected value.<br>**Command mode**: Global configuration |
| **default access-control list <***ACL number***> re-mark** | Resets the update DSCP parameters to their default values.<br>**Command mode**: Global configuration |
| **show access-control list <***ACL number***> re-mark** | Displays the current ACL re-mark parameters.<br>**Command mode**: All |

## ACL Re-Mark Update User Priority configuration

The following table describes the Update User Priority Configuration commands.

Table 163 ACL Update User Priority Configuration commands

| Command | Description |
|---|---|
| **[no] access-control list <***ACL number***> re-mark in-profile dot1p <***0-7***>** | Defines 802.1p value. The value is the priority bits information in the packet structure.<br>**Command mod**e: Global configuration |
| **[no] access-control list <***ACL number***> re-mark in-profile use-tos-precedence** | Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value. The default is disabled.<br>**Command mode**: Global configuration |
| **default access-control list <***ACL number***> re-mark** | Resets these settings to their default values.<br>**Command mode**: Global configuration |
| **show access-control list <***ACL number***> re-mark** | Displays the current ACL re-mark parameters.<br>**Command mode**: All |

## ACL Re-mark Out-of-Profile configuration

The following table describes the Re-mark Out-of-Profile Configuration commands.

Table 164 ACL Re-mark Out-of-Profile Configuration commands

| Command | Description |
|---|---|
| **[no] access-control list <***ACL number***> re-mark out-profile dscp <***0-63***>** | Sets the DiffServ Code Point (DSCP) of Out-of-Profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets.<br>**Command mode**: Global configuration |
| **default access-control list <***ACL number***> re-mark** | Resets the update DSCP parameters for Out-of-Profile packets to their default values.<br>**Command mode**: Global configuration |
| **show access-control list <***ACL number***> re-mark** | Displays the current ACL re-mark parameters.<br>**Command mode:** All |

## ACL Group configuration

These commands allow you to compile one or more ACLs into an ACL Group. Once you create an ACL Group, you can assign the ACL Group to one or more ports.

The following table describes the ACL Group Configuration commands.

Table 165 ACL Group Configuration commands

| Command | Description |
|---|---|
| **access-control group <***ACL group number***> list <***ACL number***>** | Adds the selected ACL to the ACL Group.<br>**Command mode:** Global configuration |
| **no access-control group <***ACL group number***> list <***ACL number***>** | Removes the selected ACL from the ACL Group.<br>**Command mode:** Global configuration |
| **show access-control group <***ACL group number***>** | Displays the current ACL group parameters.<br>**Command mode:** All |

# Remote Monitoring configuration

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 1757.

The following table describes the RMON Configuration commands.

Table 166 RMON commands

| Command | Description |
|---|---|
| **show rmon** | Displays the current RMON configuration.<br>**Command mode:** All |

## RMON history configuration

The switch supports up to five History Groups.

The following table describes the RMON History commands.

Table 167 RMON History commands

| Command | Description |
|---|---|
| **rmon history** *<1-65535>* **interface-oid** *<1-127 characters>* | Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows: 1.3.6.1.2.1.2.2.1.1.x<br>The interface OID can have a maximum of 127 characters.<br>**Command mode:** Global configuration |
| **rmon history** *<1-65535>* **requested-buckets** *<1-65535>* | Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved.<br>The range is from 1 to 65535. The default is 30.<br>**Note**: The maximum number of buckets that can be granted is 50.<br>**Command mode:** Global configuration |
| **rmon history** *<1-65535>* **polling-interval** *<1-3600>* | Configures the time interval over which the data is sampled for each bucket.<br>The range is from 1 to 3600 seconds. The default value is 1800 seconds.<br>**Command mode:** Global configuration |
| **[no] rmon history** *<1-65535>* **owner** *<1-127 characters>* | Enter a text string that identifies the person or entity that uses this history index.<br>The owner can have a maximum of 127 characters.<br>**Command mode:** Global configuration |
| **no rmon history** *<1-65535>* | Deletes the selected history group.<br>**Command mode:** Global configuration |
| **show rmon history** | Displays the current RMON History parameters.<br>**Command mode:** All |

## RMON event configuration

The following table describes the RMON Event commands.

Table 168 RMON Event commands

| Command | Description |
|---|---|
| **rmon event** *<1-65535>* **description** *<1-127 characters>* | Enter a text string to describe the event.<br>The description can have a maximum of 127 characters.<br>**Command mode:** Global configuration |
| **[no] rmon event** *<1-65535>* **type {log\|trap\|both}** | Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station.<br>**Command mode:** Global configuration |
| **[no] rmon event** *<1-65535>* **owner** *<1-127 characters>* | Enter a text string that identifies the person or entity that uses this event index.<br>The owner can have a maximum of 127 characters.<br>**Command mode:** Global configuration |
| **no rmon event** *<1-65535>* | Deletes this event index.<br>**Command mode:** Global configuration |

Table 168 RMON Event commands

| Command | Description |
|---|---|
| **show rmon event** | Displays the current RMON Event parameters.<br>**Command mode:** All |

## RMON alarm configuration

The Alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed.

The following table describes the RMON Alarm commands.

Table 169 RMON Alarm commands

| Command | Description |
|---|---|
| **rmon alarm** *<1-65535>* **oid** *<1-127 characters>* | Configures an alarm MIB Object Identifier.<br>The alarm OID can have a maximum of 127 characters.<br>**Command mode:** Global configuration |
| **rmon alarm** *<1-65535>* **interval** *<1-65535>* | Configures the time interval over which data is sampled and compared with the rising and falling thresholds.<br>The range is from 1 to 65535 seconds. The default is 1800 seconds.<br>**Command mode:** Global configuration |
| **rmon alarm** *<1-65535>* **sample {abs\|delta}** | Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows:<br>abs: absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.<br>delta: delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds. The default is abs.<br>**Command mode:** Global configuration |
| **rmon alarm** *<1-65535>* **alarm-type {rising\|falling\|either}** | Configures the alarm type as rising, falling, or either (rising or falling). The default is either.<br>**Command mode:** Global configuration |
| **rmon alarm** *<1-65535>* **rising-limit** *<-2147483647 to 2147483647>* | Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. The default value is 0.<br>**Command mode:** Global configuration |
| **rmon alarm** *<1-65535>* **falling-limit** *<-2147483647 to 2147483647>* | Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. The default value is 0.<br>**Command mode:** Global configuration |
| **rmon alarm** *<1-65535>* **rising-crossing-index** *<0-65535>* | Configures the rising alarm event index that is triggered when a rising threshold is crossed.<br>The range is from 0 to 65535. The default value is 0.<br>**Command mode:** Global configuration |
| **rmon alarm** *<1-65535>* **falling-crossing-index** *<0-65535>* | Configures the falling alarm event index that is triggered when a falling threshold is crossed.<br>The range is from 0 to 65535. The default value is 0.<br>**Command mode:** Global configuration |
| **[no] rmon alarm** *<1-65535>* **owner** *<1-127 characters>* | Enter a text string that identifies the person or entity that uses this alarm index.<br>The owner can have a maximum of 127 characters.<br>**Command mode:** Global configuration |
| **no rmon alarm** *<1-65535>* | Deletes this alarm index.<br>**Command mode:** Global configuration |
| **show rmon alarm** | Displays the current RMON Alarm parameters.<br>**Command mode:** All |

# Port mirroring

Port Mirroring is used to configure, enable, and disable the monitored port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage. Port mirroring is disabled by default.

NOTE: See the “Troubleshooting tools” appendix in the *N8406-023 1Gb Intelligent L3 Switch Application Guide* for information on how to use port mirroring.

The following table describes the Port Mirroring Configuration commands.

Table 170 Port Mirroring Configuration commands

| Command | Description |
|---|---|
| **[no] port-mirroring enable** | Enables or disables port mirroring. The default is disabled.<br>**Command mode:** Global configuration |
| **show port-mirroring** | Displays current settings of the mirrored and monitoring ports.<br>**Command mode:** All |

# Port-based port mirroring

The following table describes the port-based Port Mirroring Configuration commands.

Table 171 Port Mirroring Configuration commands

| Command | Description |
|---|---|
| **port-mirroring monitor-port** *<port number>* **mirroring-port** *<port number>* **{in\|out\|both}** | Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because:<br>• If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the mirrored port.<br>• If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.<br>**Command mode:** Global configuration |
| **no port-mirroring monitor-port** *<port number>* **mirroring-port** *<port number>* | Removes the mirrored port.<br>**Command mode:** Global configuration |
| **no port-mirroring monitor-port** *<port number>* | Deletes this monitor port.<br>**Command mode:** Global configuration |
| **show port-mirroring** | Displays the current settings of the monitoring port.<br>**Command mode:** All |

# Uplink Failure Detection configuration

Uplink Failure Detection (UFD) supports network fault tolerance in network adapter teams. Use these commands to configure four Failure Detection Pair of one Links to Monitor (LtM) group and one Links to Disable (LtD) group. When UFD is enabled and a Failure Detection Pair is configured, the switch automatically disables ports in the LtD if it detects a failure in the LtM. The failure conditions which are monitored in the LtM group include port link state moving to down, or port state moving to Blocking if Spanning Tree Protocol is enabled.

The following table describes the Uplink Failure Detection (UFD) Configuration commands.

Table 172 Uplink Failure Detection Configuration commands

| Command | Description |
|---|---|
| **ufd enable** | Globally turns Uplink Failure Detection ON.<br>**Command mode:** Global configuration |
| **no ufd enable** | Globally turns Uplink Failure Detection OFF. The default is OFF.<br>**Command mode:** Global configuration |
| **ufd fdp** *<fdp number>* | Enter FDP configuration mode for the selected number.<br>**Command mode:** Global configuration |
| **show ufd** | Displays the current Uplink Failure Detection configuration parameters.<br>**Command mode:** All |

## Failure Detection Pair configuration

Use these commands to configure a Failure Detection Pair, which consists of one Link to Monitor (LtM) and one Link to Disable (LtD). When the switch detects a failure on the LtM, it automatically disables the ports in the LtD.

The following table describes the Failure Detection Pair (FDP) configuration commands.

Table 173 Failure Detection Pair Configuration commands

| Command | Description |
|---|---|
| **enable** | Enables the FDP Parameters.<br>**Command mode:** FDP configuration |
| **no enable** | Disables the FDP Parameters. The default is disabled.<br>**Command mode:** FDP configuration |

## Link to Monitor configuration

The following table describes the Link to Monitor (LtM) commands. The LtM can consist of only one uplink port (ports 20-24), a single trunk containing only uplink ports, or a single LACP trunk containing only uplink ports.

Table 174 Link to Monitor commands

| Command | Description |
|---|---|
| **ltm port** *<port number>* | Adds a port to the LtM. Only uplink ports (20-24) are allowed in the LtM.<br>**Command mode:** FDP configuration |
| **no ltm port** *<port number>* | Removes a port from the LtM.<br>**Command mode:** FDP configuration |
| **ltm portchannel** *<1-12>* | Adds a trunk group to the LtM. The LtM trunk group can contain only uplink ports (20-24).<br>**Command mode:** FDP configuration |
| **no ltm portchannel** *<1-12>* | Removes a trunk group from the LtM.<br>**Command mode:** FDP configuration |
| **ltm adminkey** *<1-65535>* | Adds a LACP trunk group to the LtM. Defines a adminkey configured to a LACP trunk group. The LtM LACP trunk group can contain only uplink ports (20-24).<br>**Command mode:** FDP configuration |
| **no ltm adminkey** *<1-65535>* | Removes a LACP trunk group from the LtM.<br>**Command mode:** FDP configuration |

# Link to Disable configuration

The following table describes the Link to Disable (LtD) commands. The LtD can consist of any mix of downlink ports (ports 1-16) and trunk groups that contain only downlink ports and LACP trunk groups that contain only downlink ports.

Table 175 Link to Disable commands

| Command | Description |
|---|---|
| **ltd port** *<port number>* | Adds a port to the current LtD group. Only downlink ports (1-16) are allowed in the LtD.<br>**Command mode:** FDP configuration |
| **no ltd port** *<port number>* | Removes a port from the current LtD group.<br>**Command mode:** FDP configuration |
| **ltd portchannel** *<1-12>* | Adds a trunk group to the current LtD group. LtD trunk groups can contain only downlink ports (1-16).<br>**Command mode:** FDP configuration |
| **no ltd portchannel** *<1-12>* | Removes a trunk group from the current LtD group.<br>**Command mode:** FDP configuration |
| **ltd adminkey** *<1-65535>* | Adds a LACP trunk group to the current LtD group. Defines a adminkey configured to a LACP trunk group. LtD LACP trunk groups can contain only downlink ports (1-16).<br>**Command mode:** FDP configuration |
| **no ltd adminkey** *<1-65535>* | Removes a LACP trunk group from the current LtD group.<br>**Command mode:** FDP configuration |

# Configuration Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the prompt, enter:

```
Switch(config)# show running-config
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches. Paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via FTP/TFTP.

# Saving the active switch configuration

When the **`copy running-config {tftp|ftp}`** command is used, the active configuration commands of the switch will be uploaded to the specified script configuration file on the TFTP/FTP server. To start the switch configuration upload, at the prompt, enter:

```
Switch(config)# copy running-config {tftp|ftp}
```

NOTE: The output file is formatted with line-breaks but no carriage returns. The file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).

NOTE: If the TFTP server is running SunOS™ or the Solaris™ operating system, the specified file must exist prior to executing the `copy running-config tftp` command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

# Restoring the active switch configuration

When the **`copy {tftp|ftp} running-config`** command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial configuration.

To start the switch configuration download, at the prompt, enter:

```
Switch(config)#  copy {tftp|ftp} running-config
```

NOTE: The switch supports three configuration files: active, backup, and factory. See the “Selecting a configuration block” section in the “Boot Options” chapter for information on how to set which configuration file to use upon boot up.

# Operations Commands

## Introduction

Operations-level commands are used for making immediate and temporary changes to switch configuration. Operations commands are used for bringing ports temporarily in and out of service. These commands are available only from an administrator and operator login.

The following table describes basic Operations commands. The following sections provide more detailed information and commands.

Table 176 Operations commands

| Command | Description |
|---|---|
| **password** | Allows the user to change the password. You need to enter the current password in use for validation.<br>**Command mode**: All |
| **clear logging** | Clears all Syslog messages. This command is available only from an administrator login.<br>**Command mode**: Privileged EXEC |
| **ntp send** | Allows the user to send requests to the NTP server. This command is available only from an adminstrator login.<br>**Command mode**: Privileged EXEC |

## Operations-level port options

Operations-level port options are used for temporarily disabling or enabling a port.

Table 177 Operations-Level Port commands

| Command | Description |
|---|---|
| **[no] interface gigabitethernet** *<port number>* **rmon** | Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function.<br>**Command mode**: All |
| **no interface gigabitethernet** *<port number>* **shutdown** | Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reloaded.<br>**Note**: This command does not enable a port that has been disabled by an ekeying mismatch error.<br>**Command mode**: All |
| **interface gigabitethernet** *<port number>* **shutdown** | Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reloaded.<br>**Command mode**: All |
| **show interface gigabitethernet** *<port number>* **operation** | Displays the current settings for the port.<br>**Command mode**: All |

## Operations-level port 802.1x options

Operations-level port 802.1x options are used to temporarily set 802.1x parameters for a port.

Table 178 Operations-Level Port 802.1x commands

| Command | Description |
|---|---|
| **interface gigabitethernet <***port number***> dot1x init** | Re-initializes the 802.1x access-control parameters for the port. The following actions take place,depending on the 802.1x port configuration:<br>• **force unauth** - the port is placed in unauthorized state, and traffic is blocked.<br>• **auto** - the port is placed in unauthorized state, then authentication is initiated.<br>• **force auth** - the port is placed in authorized state, and authentication is not required.<br>**Command Mode**: All |

Table 178 Operations-Level Port 802.1x commands

| Command | Description |
|---|---|
| **interface gigabitethernet {<*port number*>} dot1x re-authenticate** | Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1x mode is configured as `auto`.<br>**Command Mode**: All |

## Operations-level VRRP options

Operations-level VRRP options are described in the following table.

Table 179 Operations-Level VRRP commands

| Command | Description |
|---|---|
| **router vrrp backup <***1-255***>** | Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases:<br>• This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same)<br>• This switch's virtual router has a higher priority and preemption is enabled.<br>• There are no other virtual routers available to take master control.<br>**Command Mode**: All |

# Boot Options

## Introduction

You must be logged in to the switch as the administrator to use the Boot Options commands.

The Boot Options allow you to perform the following functions:

- Select a switch software image to be used when the switch is next reloaded.
- Select a configuration block to be used when the switch is next reloaded.
- Download or upload a new software image to the switch via FTP/TFTP.

Each of the Boot Options commands is discussed in the following sections.

## Updating the switch software image

The switch software image is the executable code running on the switch. A version of the image ships with the switch, and comes pre-installed on the switch. As new versions of the image are released, you can upgrade the software running on the switch.

To upgrade the software image on the switch:

- Load the new image onto a FTP/TFTP server on your network.
- Download the new image from the FTP/TFTP server to the switch.
- Select the new software image to be loaded into switch memory the next time the switch is reloaded.

### Downloading new software to the switch

The switch can store up to two different software images, called image1 and image2, as well as boot software, called boot. When you download new software, you must specify where it should be placed: either into image1, image2, or boot.

For example, if your active image is currently loaded into image1, you would probably load the new image software into image2. This lets you test the new software and reload the original active image (stored in image1), if needed.

To download new software to the switch, you need the following:

- The image or boot software loaded on a FTP/TFTP server on your network
- The hostname or IP address of the FTP/TFTP server
- The user name and password for FTP server, if necessary
- The name of the new software image or boot file

NOTE: The DNS parameters must be configured if specifying hostnames. See the “Domain name system configuration” section in the “Configuration Commands” chapter.

When the above requirements are met, use the following procedure to download the new software to the switch.

1. In Privileged EXEC mode, enter:

```
Switch# copy tftp {image1|image2|boot-image}
```

or

```
Switch# copy ftp {image1|image2|boot-image}
```

2. Enter the name of the switch software to be replaced:

```
Enter name of switch software image to be replaced
 ["image1"/"image2"/"boot"]: <image>
```

3. Enter the hostname or IP address of the FTP/TFTP server:

```
Address or name of remote host: <server name or IP address>
```

4. Enter the name of the new software file on the server:

```
Source file name: <filename>
```

The exact form of the name will vary by TFTP server. However, the file location is normally relative to the FTP or TFTP directory.

5. Enter the user name, if you are using a FTP server:

```
Enter username for FTP server or hit return for TFTP server: <userID>
```

6. Enter the password for the FTP server (if prompted):

```
Enter password for username on FTP server: <password>
```

7. The system prompts you to confirm your request.

   You should next select a software image to run, as described in the “Selecting a Soft Image to Run” section.

8. If you are loading an image from which you are not currently booted, the system prompts you to change the image.

```
image2 currently contains Software Version 1.0.0
 that was downloaded at 15:46:36 Wed Apr 23, 2006.
New download will replace image2 with file "1.1.0_OS.img"
 from TFTP server 192.168.2.4.
Confirm download operation [y/n]: y
Invoking TFTP over port 69...
Starting download...
File appears valid
Download in
progress..................................................
Image download complete (1333953 bytes)
Writing to flash...This takes about 90 seconds. Please wait
Write complete (1333953 bytes), now verifying FLASH...
Verification of new image2 in FLASH successful.
image2 now contains Software Version 1.1.0
Switch is currently set to boot software image1.
Do you want to change that to the new image2? [y/n] y
Next boot will use new software image2.
```

# Selecting a software image to run

You can select which software image (image1 or image2) you want to run in switch memory for the next reboot.

1. In Global Configuration mode, enter:

```
Switch(config)# boot image {image1|image2}
```

2. Enter the name of the image you want the switch to use upon the next boot. The system informs you of which image is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use switch software "image1" on next reset.

Specify new image to use on next reset ["image1"/"image2"]:
```

# Uploading a software image from the switch

You can upload a software image from the switch to a FTP or TFTP server.

1. In Privileged EXEC mode, enter:

```
Switch# copy {image1|image2|boot-image} tftp
```

   or

```
Switch# copy {image1|image2|boot-image} ftp
```

2. The system prompts you for information. Enter the desired image:

```
Enter name of switch software image to be uploaded

["image1"|"image2"|"boot"]: <image>
```

3. Enter the name or the IP address of the FTP/TFTP server:

```
Address or name of remote host: <server name or IP address>
```

4. Enter the name of the file into which the image will be uploaded on the FTP/TFTP server:

```
Destination file name: <filename>
```

5. Enter the user name, if you are using a FTP server:

```
Enter username for FTP server or hit return for TFTP server: <userID>
```

6. Enter the password for the FTP server (if prompted):

```
Enter password for username on FTP server: <password>
```

7. The system then requests confirmation of what you have entered. To have the file uploaded, enter y.

```
image2 currently contains Software Version 1.1.0
Upload will transfer image2 (1889411 bytes) to file "test"
 on TFTP server 192.1.1.1.
Confirm upload operation [y/n]: y
```

# Selecting a configuration block

When you make configuration changes to the switch, you must save the changes so that they are retained beyond the next time the switch is reset. When you execute a save operation (**copy running-config startup-config**), your new configuration changes are placed in the active configuration block. The previous configuration is copied into the backup configuration block.

There is also a factory configuration block. This holds the default configuration set by the factory when the switch was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured switch is moved to a network environment where it will be re-configured for a different purpose.

Use the following procedure to set which configuration block you want the switch to load the next time it is reset:

1. In Global Configuration mode, enter:

```
Switch(config)# boot configuration-block {active|backup|factory}
```

2. Enter the name of the configuration block you want the switch to use.

   The system indicates which configuration block is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use active configuration block on next reset.

Specify new block to use ["active"/"backup"/"factory"]:
```

# Resetting the switch

You can reset the switch to make your software image file and configuration block changes occur.

Resetting the switch causes the Spanning Tree Protocol to restart. This process can be lengthy, depending on the topology of your network.

To reset the switch, at the prompt, enter:

```
>> Switch# reload
```

You are prompted to confirm your request.

To display current boot options, enter:

```
>> Switch# show boot
```

# Accessing the AOS CLI

To access the AOS CLI, enter the following command from the ISCLI, and reload the switch:

```
>> Switch(config)# boot cli-mode aos
```

The default command-line interface for this switch is the AOS CLI. To access the ISCLI, enter the following command and reset the switch:

```
Main# boot/mode iscli
```

Users can select the CLI mode upon login, if the following command is enabled:
`boot cli-mode prompt`

Only an administrator connected through the console port can view and enable the `prompt` command. When `prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

# Maintenance Commands

## Introduction

The Maintenance commands are used for debugging purposes, enabling you to generate a technical support dump of the critical state information in the switch, and to clear entries in the Forwarding Database and the Address Resolution Protocol (ARP) and routing tables. These commands are available only from an administrator login.

Dump information contains internal switch state data that is written to flash memory on the switch after any one of the following occurs:

- The switch administrator forces a switch panic. The panic option causes the switch to dump state information to flash memory, and then causes the switch to reboot.
- The switch administrator enters the switch reset key combination (`Ctrl-Shift-6`) on a device that is attached to the console port.
- The switch detects a hardware or software problem that requires a reboot.

The following sections provide detailed information and commands.

### System maintenance

The System Maintenance commands are reserved for use by NEC technical support. The options are used to perform system debugging.

The following table describes the System Maintenance commands.

Table 180 System Maintenance commands

| Command | Usage |
|---|---|
| **debug debug-flags** | Sets the flags that are used for debugging purposes by NEC technical support.<br>**Command mode:** All except User EXEC |

### Forwarding Database maintenance

The Forwarding Database (FDB) Manipulation commands can be used to view information and to delete a MAC address from the Forwarding Database or clear the entire Forwarding Database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

The following table describes the FDB Manipulation commands.

Table 181 FDB Manipulation commands

| Command | Usage |
|---|---|
| **show mac-address-table address** *<MAC address>* | Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using one of the following:<br>• xx:xx:xx:xx:xx:xx format (for example: 08:00:20:12:34:56)<br>• xxxxxxxxxxxx format (for example: 080020123456).<br>**Command mode:** All |
| **show mac-address-table port** *<port number>* | Displays all FDB entries for a particular port.<br>**Command mode:** All |
| **show mac-address-table vlan** *<1-4095>* | Displays all FDB entries on a single VLAN.<br>**Command mode:** All |
| **show mac-address-table** | Displays all entries in the Forwarding Database.<br>**Command mode:** All |
| **clear mac-address-table** | Clears the entire Forwarding Database from switch memory, then adds the static entries to the Forwarding Database.<br>**Command mode:** All except User EXEC |

## Debugging options

The Miscellaneous Debug commands display trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using Debug commands:

- Events traced by the management processor (MP)
- Events traced to a buffer area when a reset occurs

If the switch resets for any reason, the management processor (MP) trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by NEC technical support.

The following table describes the Miscellaneous Debug commands:

Table 182 Miscellaneous Debug commands

| Command | Usage |
|---|---|
| **debug mp-trace** | Displays the management processor trace buffer. Header information similar to the following is shown:<br>MP trace buffer at 13:28:15 Fri May 25, 2002; mask: 0x2ffdf748<br>The buffer information is displayed after the header.<br>**Command mode:** All except User EXEC |
| **debug mp-snap** | Displays the management processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred.<br>**Command mode:** All except User EXEC |
| **clear flash-config** | Deletes all flash configuration blocks. The next time the switch is rebooted, it returns to the factory default settings.<br>**Command mode:** All except User EXEC |

## ARP cache maintenance

The following table describes the Address Resolution Protocol commands:

Table 183 ARP Maintenance commands

| Command | Usage |
|---|---|
| **show ip arp find** *<IP address>* | Shows a single ARP entry by IP address.<br>**Command mode:** All except User EXEC |
| **show ip arp interface** *<port number>* | Shows ARP entries on a single port.<br>**Command mode:** All except User EXEC |
| **show ip arp vlan** *<1-4095>* | Shows ARP entries on a single VLAN.<br>**Command mode:** All except User EXEC |
| **show ip arp reply** | Shows the list of IP addresses that the switch will respond to for ARP requests.<br>**Command mode:** All except User EXEC |
| **show ip arp** | Shows all ARP entries.<br>**Command mode:** All except User EXEC |
| **clear ip arp-cache** | Clears the entire ARP list from switch memory.<br>**Command mode:** All except User EXEC |

NOTE: To display all ARP entries currently held in the switch, or a portion according to one of the commands listed above, see the “ARP information” section of the “Information Commands” chapter.

## IGMP Snooping maintenance

The following table describes the IGMP Snooping Maintenance commands.

Table 184 IGMP Snooping Maintenance commands

| Command | Usage |
|---|---|
| **show ip igmp groups address** *<IP address>* | Shows a single IGMP Multicast group by IP address.<br>**Command mode:** All except User EXEC |
| **show ip igmp groups vlan** *<1-4094>* | Shows IGMP Multicast groups on a single VLAN.<br>**Command mode:** All except User EXEC |
| **show ip igmp groups interface** *<port number>* | Shows IGMP Multicast groups on a single port.<br>**Command mode:** All except User EXEC |
| **show ip igmp groups** | Shows all IGMP Multicast groups.<br>**Command mode:** All except User EXEC |
| **clear ip igmp snoop** | Clears IGMP Multicast data from switch memory.<br>**Command mode:** All except User EXEC |

## IGMP Mrouter maintenance

The following table describes the IGMP Multicast Routers Maintenance commands.

Table 185 IGMP Multicast Group Maintenance commands

| Command | Usage |
|---|---|
| **show ip igmp groups vlan** *<1-4094>* | Shows IGMP Multicast groups on a single VLAN.<br>**Command mode:** All except User EXEC |
| **show ip igmp mrouter** | Shows all IGMP Multicast routers.<br>**Command mode:** All except User EXEC |
| **clear ip igmp mrouter** | Clears IGMP Multicast router data from switch memory.<br>**Command mode:** All except User EXEC |

## Technical support dump

**show tech-support**

**Command mode:** All

Use the dump command to dump all switch information, statistics, and configuration for technical support.

If you want to capture dump data to a file, set the communication software on your workstation to capture session data prior to issuing the dump commands.

## TFTP/FTP technical support dump put

Use this command to put (save) the technical support dump to a TFTP server.

To save dump information via TFTP, at the prompt, enter:

```
Switch# copy tech-support tftp
```

or

To save dump information via FTP, at the prompt, enter:

```
Switch# copy tech-support ftp
```

The system prompts you to enter the server IP address or hostname, and the target dump file name.

## Uuencode flash dump

**show flash-dump-uuencode**

**Command mode**: All

Using this command, dump information is presented in uuencoded format. This format makes it easy to capture the dump information as a file or a string of characters.

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the command. This will ensure that you do not lose any information. Once entered, the command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the above command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see the "Clearing dump information" section later in this chapter.

To access dump information, at the prompt, enter:

```
Switch# show flash-dump-uuencode
```

The dump information is displayed on your screen and, if you have configured your communication software to do so, captured to a file. If the dump region is empty, the following displays:

```
No FLASH dump available.
```

## TFTP/FTP system dump put

Use this command to put (save) the system dump to a TFTP/FTP server.

NOTE: If the TFTP server is running SunOS or the Solaris operating system, the specified **copy flash-dump tftp** (or ftp) file must exist prior to executing the **copy flash-dump tftp** command (or **copy flash-dump ftp**) command, and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via TFTP, at the prompt, enter:

```
Switch# copy flash-dump tftp
```

or

To save dump information via FTP, at the prompt, enter:

```
Switch# copy flash-dump ftp
```

The system prompts you to enter the server IP address or hostname, and the target dump file name.

## Clearing dump information

To clear dump information from flash memory, at the prompt, enter:

```
Switch# clear flash-dump
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

## Panic command

The panic command causes the switch to dump state information immediately to flash memory and reboot.

To select panic, at the prompt, enter:

```
>> Switch# debug panic
A FLASH dump already exists.
Confirm replacing existing dump and reboot [y/n]:
```

Enter **y** to confirm the command:

```
Dump and reboot [y/n]: y
```

A list of messages is displayed:

```
Starting system dump...done.

Reboot at 11:54:08 Wednesday October 30, 2006...

. . . . . .

. . . . . .

Rebooted because of console PANIC command.

Booting complete
```

# Unscheduled system dumps

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Wednesday October 30, 2006.
      Use show flash-dump uuencode to
      extract the dump for analysis and clear flash-dump to
     clear the FLASH region. The region must be cleared
     before another dump can be saved.
```